Montgomery County, Maryland

Office of the County Executive

Office of Internal Audit

Information Technology Risk Assessment

February 19, 2020

MCIA-20-5

TABLE OF CONTENTS

Background

This report summarizes the objectives, background, and approach of the Information Technology (IT) Risk Assessment (assessment) performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County (the County) Office of Internal Audit (MCIA). The assessment provides the County with information as to the types of IT risks that are present and identifies the maturity of policies, procedures, and controls defined to mitigate those risks.

The assessment will allow the County to enhance and build upon its Information Security Program, formulate recommendations to improve or enhance key security controls, and identify a proposed audit plan to include recommended audits in the audit universe to be executed per fiscal year.

The assessment's objectives were to:

1. Assess and prioritize the County's current IT risk environment
2. Establish a new IT specific internal audit plan designed to address the County's most significant IT risks

The assessment was conducted in three phases from January 2019 to November 2019 and included identification and assessment of IT domains specific to the Department of Technology Services (DTS) and decentralized IT functions within individual County departments. The assessment included survey, inquiry, and inspection procedures to assess and prioritize the County's current IT risk environment. The results were evaluated to identify risks that appear to exist individually and across multiple departments and may represent County-wide risks that should be considered and addressed.

County-wide Information Technology Overview

Montgomery County leverages the use of information technology through a combination of centralized and decentralized functions to enable employees to provide quality services to citizens and businesses, deliver information and services to citizens at work, at home, and in the community, and increase the productivity of government and citizens.

Centralized IT Functions

DTS is comprised of four operating divisions and multiple offices and programs providing Enterprise Technology services to all County departments and offices. Listed below are the DTS operating divisions:

- Enterprise Applications and Solutions Division (EASD)
- Enterprise Telecommunications Services Division (ETSD)
- Enterprise Systems and Operations Division (ESOD)
- Enterprise Resource Planning Division (ERPD)
- Office of Broadband Programs (OBP)

Decentralized IT Functions

DTS provides certain information technology services and communication services necessary supporting the daily operation of Montgomery County departments. Further, each individual department functions as a complete information technology entity providing evaluation and implementation of advanced data, applications, teleprocessing, and radio systems. Department Information Technology teams are responsible for identifying and managing these advanced approaches for the ongoing operation and growth of Montgomery County departments.

Scope and Methodology

The following provides an overview of the assessment methodology followed in identifying and assessing these IT and security related risks, and developing County, DTS and departmental heat maps.

This assessment was not conducted as an assurance audit, therefore it did not include detailed testing of internal controls. Rather, the intent of this assessment is to inform senior management of high-level risks within the County's IT environment, and to assess the perceived maturity of the current control environment designed to address and mitigate associated risks.

Given the sensitive and confidential nature of IT risks identified as a result of this assessment, the details of the specific risk scenarios are not provided as part of this report. These details have been shared with the responsible core department and business offices so that they may develop and take appropriate corrective actions to strengthen the control processes and systems applicable to the risk scenarios.

We recognize the importance of completely understanding the County's IT control environment, as it dramatically impacts the operation of nearly every department. Risks associated with a failure in IT will result in significant disruption of the County's day-to-day operations unless there are proper procedures and controls embedded within the operations. In order to understand the County's IT control environment, and ensure that the universe of countywide IT processes, applications, and associated risks can be considered, the assessment focused on identifying and evaluating the audit areas specific to each of the following:

- DTS operating divisions
- The decentralized IT functions within individual County departments

To assess controls, SC&H leveraged a tailored methodology, combining National Institute of Standards and Technology ("NIST") 800-53[1] and the Federal Information Security Modernization Act of 2014 (FISMA)[2] security frameworks as a benchmark to determine areas of risk and best practice objectives. The following is a description of domains assessed within the IT Risk Assessment.

[1] https://nvd.nist.gov/800-53

[2] https://www.dhs.gov/sites/default/files/publications/Final%20FY%202018%20IG%20FISMA%20Metrics%20v1.0.1.pdf

1. **IT Governance/Risk Management**
   Organization's approach to reliably achieve planned objectives while following the established mission and business goals.
2. **Organizational Structure**
   Activities that support the allocations of responsibilities for specific processes, functions, and responsibilities to internal and external personnel.
3. **Personnel Management**
   Management of personnel through succession planning, background checks, training for specific roles and responsibilities, and monitoring for training requirements.
4. **Budgeting Process**
   Organization's approach on establishing budget line items for information technology investments, systems, and services.
5. **IT Policies and Procedures**
   Establishment and implementation of the fundamental baseline requirements adopted by the organization in which information technology functions and processes must follow.
6. **Vendor Management**
   The organization's approach to ensure specific service and risk levels, at a specified cost, are being managed for contracted services.
7. **Asset Management**
   Management and inventory of information technology items (hardware, software, network devices, etc.) and the associated ownership, acceptable use, and return of the items.
8. **Data Security**
   The protection, classification, and control of sensitive data and media containing sensitive data (both paper and digital).
9. **Monitoring**
   Observing and measuring information technology devices, applications, and equipment to be aware of the state of operations (uptime, downtime, capacity, and violations).
10. **Physical Security**
    Organization's approach to deter, prevent, monitor, and detect physical access violations to secured facilities including magnetic badge readers, biometric devices, electronic keypad access control, proximity access control, and electronic locks.
11. **IT Security**
    The strategies developed to prevent unauthorized access to organizational assets such as computers, networks, and data, while maintaining integrity, confidentiality, and availability of sensitive information.
12. **Configuration Management**
    Organization's approach on establishing and enforcing security configuration settings for information systems, process for connecting new systems to the environment, and assessing the security impact of changes prior to implementation into production.
13. **Application Management**

Administration of granting individual users and groups, within a system, access to internal and external applications through permissions and security requirements.

14. **Computer Operations**
    Organization's approach on conducting, testing, and restoring backups of user-level and system-level information contained in information systems.
15. **Response Planning**
    Incident response and disaster recovery strategies used to minimize the impact from security breaches, security incidents, and business interruptions to business operations.
16. **Risk Assessment**
    The organizations approach for identifying and managing security vulnerabilities, threats, and overall risk and association with the organization established risk tolerance level.

The assessment was conducted in three phases as summarized below. Each IT process was risk-ranked by the evaluation of risk factors using the compilation of information and data gathered during the assessment phases.

1. Phase 1: Scoping and preliminary departmental assessment including surveys and interviews
2. Phase 2: Data collection and fieldwork including in-depth interviews, review of related policies and procedures, and assessment of risks/maturity
3. Phase 3: Analysis and reporting including development of Risk Assessment report, Management Advisory Letter, Proposed Audit Plan, and delivery of respective heat maps

Information was gathered by reviewing pertinent documents and reports, conducting interviews with management and process owners, administering surveys, and observing select activity.

SC&H administered, received, and reviewed surveys and conducted interviews during Phase 1 across 34 departments to gain a comprehensive understanding of the ownership and application of IT domains unique to their specific IT environment. SC&H evaluated and risk ranked each of the 34 departments across 17 IT/Security areas of focus and calculated an average risk score used for down selecting departments for Phase 2 review.

Based on the risk rankings calculated during Phase 1, select departments were chosen along with certain DTS operating divisions, for additional review procedures. During Phase 2, SC&H conducted in depth interviews across 21 select departments, offices, and organizational units as well as performed review of existing relevant policies and procedures. SC&H created a list of key processes by department and assess conformity across IT domains to the organizations risk tolerance. SC&H evaluated departmental security strategies and supporting programs to identify areas of high risk that would benefit from risk-based auditing.

Heat Map Approach and Content

SC&H was also tasked with developing both a county-wide IT Risk Assessment heat map as well as individual offices and departmental IT Risk Assessment heat maps. A heat map is a tool

used to present the results of a risk assessment process visually and in a meaningful and concise way.

Assessing the likelihood and impact of each potential IT risk is a subjective process. SC&H assessed the County's risk tolerance, based on discussions with management and our industry knowledge and expertise to assign risk scores to risk ratings and determine the appropriate level of response for each risk.

The term "Risk" is defined by NIST[3] as follows:

> *Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:*
>
> *(i) the adverse impacts that would arise if the circumstance or event occurs; and*
>
> *(ii) the likelihood of occurrence.*
>
> *Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur.*

Additionally, we identified areas that deserve the most attention and evaluated them relative to the Control Ranking, the Likelihood (Probability) of a risk event occurring, and the Impact it may have on the organization. These risk frameworks are based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework.

Figure 1 below describes each level in the Likelihood ranking scheme. ***Figure 2*** describes each level in the Impact ranking scheme. ***Figure 3*** describes the calculation for Overall Risk Ranking.

LIKELIHOOD			
		Annual Frequency	**Annual Probability**
1	**Rare**	The risk event occurs yearly or less than one time per year.	10% chance of occurrence
2	**Occasional**	The risk event occurs more than yearly to monthly.	10% - 35% chance of occurrence
3	**Reasonably Frequent**	The risk event occurs more than monthly to weekly.	35% - 65% chance of occurrence

[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Page 6)

4	Frequent	The risk event occurs more than weekly to daily.	65% - 90% chance of occurrence
5	Very Frequent	The risk event occurs multiple times a day.	> 90% chance of occurrence

***Figure 1**. Ranking Scheme for Likelihood (Probability)*

IMPACT				
		Financial Loss	Media Coverage	Employee Turnover
1	Incidental	Financial loss to company < $1,000.	No media coverage	Isolated employee dissatisfaction
2	Minor	Financial loss to company $1,000 - $10,000	Limited, local media coverage	General employee morale problems
3	Moderate	Financial loss to company $10,000 - $100,000	Short-term, regional or national media coverage	Widespread employee morale problems
4	Major	Financial loss to company $100,000 - $10,000,000	National, long-term media coverage	Widespread employee morale problems and turnover
5	Catostrophic	Financial loss to company > $10,000,000	International, long-term media coverage	Widespread employee morale issues and loss of multiple senior leaders

***Figure 2**. Ranking Scheme for Impact*

Risk Ranking							
Likelihood	5	Very Frequent	Minor	Moderate	Major	Catastrophic	Catastrophic
	4	Frequent	Minor	Moderate	Major	Major	Catastrophic
	3	Reasonably Frequent	Incidental	Minor	Moderate	Major	Major
	2	Occasional	Incidental	Incidental	Minor	Moderate	Moderate
	1	Rare	Incidental	Incidental	Minor	Minor	Moderate
			Incidental	Minor	Moderate	Major	Catastrophic
			1	2	3	4	5
			Impact				

***Figure 3**. Overall Risk Ranking Calculation*

FISMA Reporting Metrics were leveraged to assess each IT domains level of maturity.

Maturity Level	Description
Level 1: Ad Hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

***Figure 4**. Assessment Maturity Model Description*

Maturity levels apply to an organization's performance and process improvement achievements in individual practice areas. Within domains, the practices are organized into practice groups labeled Level 1 to Level 5 which provide an evolutionary path to performance improvement. Each level builds on the previous levels by adding new functionality or rigor resulting in increased capability.

Summary

The results of the IT Risk Assessment (Step One) were captured through a combination of Heat Maps detailing defined risk levels and associated maturity levels by department/enterprise. The overall risk score assigned to each IT Domain was determined through a combination of the likelihood of a given threat source attempting to exercise a given vulnerability and the magnitude of the impact should a threat-source successfully exercise the vulnerability. The overall risk score does not account for the corresponding maturity and/or adequacy of planned or existing security controls for reducing or eliminating risk. Accordingly, the following areas were identified as high risk.

- IT Governance
- Personnel and Resource Management
- Disaster Recovery and Business Continuity
- Vulnerability and Incident Management
- Vendor Management
- Physical Security
- Database and System Monitoring
- Application Access Management
- Computer Operations Management (Backups)

The results of the IT Risk Assessment will be reviewed and leveraged in the development of a formal Internal Audit IT Audit Plan (Step Two). The IT Audit Plan will include recommended IT areas of focus, preliminary objectives, and associated risks as identified within the IT Risk Assessment. Through the conduct of targeted internal audits planned in Step Two, additional procedures will be performed to evaluate the effectiveness of the IT control environment, along with identifying any processes where the County should focus its efforts to strengthen and enhance the control environment.

The IT Risk Assessment provides management with information as to the types of operational risks that are present and considerations for mitigating these risks. The IT Risk Assessment report and supporting heat maps will allow Montgomery County to enhance and build upon its Information Security Program requirements and formulate recommendations to improve or enhance key security controls, develop a list of security program initiatives, and identify a prioritized list of improvements to expedite tactical and strategic organizational responses to IT security risks and events.

Appendix A – Areas of Focus

Domain	Control #	Control Description
IT Governance/Risk Management (GR)	GR-1	The organization has established a short term (1 year) and long-term (3 to 5 year) business objectives.
	GR-2	The organization has a formally documented IT Strategic Plan.
	GR-3	IT Operations is in alignment with IT Governance goals, objectives, and missions.
	GR-4	The organization requires that providers of external information system services comply with organizational information security requirements through specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs.
	GR-5	The organization has developed an incident response plan that provides a roadmap for implementing its incident response capability, investigation, reporting, and recording processes.
Organizational Structure (OZ)	OZ-1	A documented and updated organizational chart exist that shows the structure, relationship, and relative ranks of positions within IT and the overall organization.
	OZ-2	The organization has a methodology and understanding of external parties roles and responsibilities involved with co-sourcing and out-sourcing of specific functions.
	OZ-3	The organization has established a risk management process in which roles and responsibilities have been assigned to internal and external stakeholders and risk executive functions (Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders).
Personnel Management (PM)	PM-1	The organization has a succession plan process in place for identifying and developing new leaders who can replace old leaders when they are no longer available to perform job functions.
	PM-2	The organization Human Resource department manages background checks and associated methodologies, agreements, SLA's in place for hiring staffing personnel.
	PM-3	The organization provides basic security awareness training to information system users as part of initial training for new users and when required by information system changes.

	PM-4	The organization provides role-based security training to personnel with assigned roles and responsibilities before authorizing access to information systems or performing assigned duties and when required by information system changes.
	PM-5	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.
Budgeting Process (BP)	BP-1	The organization determines information security requirements for the information system or information system service in mission/business process planning.
	BP-2	The organization determines, documents, and allocates the resources required to protect the information system or information service as part of its capital planning and investment control process.
	BP-3	The organization performs a cost benefit analysis for large IT initiatives to measure the benefits gained through IT investments.
IT Policies and Procedures (PP)	PP-1	The organization develops, documents, and disseminates IT-related policies and procedures to IT personnel.
	PP-2	The organization reviews and updates the current IT-related policies and procedures on annual basis.
	PP-3	The organization assigns an owner or committee to perform reviews and updates of IT-related policies and procedures.
Vendor Management (VM)	VM-1	The organization employs a defined strategy, contracting tools, and procurement methods for the purchase of information system, system components, or information system services from suppliers.
	VM-2	The organization determines, documents, and allocates the resources required to protect the information system or information service as part of its capital planning and investment control process.
	VM-3	The organization develops, documents, and disseminates vendor management policies and procedures.
	VM-4	The organization reviews and updates the current vendor management policies and procedures on annual basis.
	VM-5	The organization manages 3rd party service providers to IT systems through: - review and evaluation of SOC reports - monitoring performance against SLAs

Asset Management (AM)	AM-1	The organization maintains a comprehensive, updated, and accurate inventory of information systems including:- IT system name- IT system description- Associated databases- Associated operating systems- Criticality rating- IT owner- Business owner
	AM-2	The organization maintains a comprehensive, updated, and accurate network diagram that includes: - All connections between sensitive data and other networks and applications - Data flow across systems and network components
	AM-3	The organization develops and documents an inventory of information system components that reflects the current information system components (hardware inventory, software license, network components/devices) and inventory specifications including component owners, serial numbers, device type, and physical location(s).
Data Security (DS)	DS-1	The organization employs a data classification scheme/methodology (i.e. “public”, “confidential”, “sensitive”, “critical”, etc.) to help guide where data is located, what access levels are implemented, and the specific protection levels that are to be implemented.
	DS-2	The organization develops, documents, and disseminates a privacy policy that is current and updated as needed.
	DS-3	The organization develops and disseminates data access agreement documents such as nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements that requires acknowledgment that individuals have read, understand, and agree to abide by the constraints.
	DS-4	The organization employs encryption methods used to protect the confidentiality and integrity of data at rest and in transit.
Monitoring (M)	M-1	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists.
	M-2	The organization conducts monitoring of databases and systems for capacity, availability, uptime, and storage.
	M-3	The organizations incident response capabilities includes monitoring of security violations that may pose a threat to the organization's environment such as failed login attempts.

	M-4	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
Physical Security (PS)	PS-1	The organization protects data center equipment from factors caused by environmental impact.
	PS-2	The organization enforces physical access authorization at entry/exit points to the facility where the information systems resides by verifying individual access authorizations before granting access to the facility and controlling ingress/egress the facility using physical access control systems/devices.
	PS-3	The organization issues authorization credentials for facility access.
IT Security (SC)	SC-1	The organization develops, documents, and disseminates an IT Security Policy and Procedure that defines: - IT Security roles and responsibilities - User account provisioning - User access removal - Periodic review of access privileges - Management of segregation of duties - Password policy, account lockout, and session lockout - Mobile device policy - Clearance procedures for new employees and contractors - Identity and authentication management - Network security - Security patches and updates
	SC-2	The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorizes remote access to the information system prior to allowing such connection.
Configuration Management (CM)	CM-1	The organization has a process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
	CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

	CM-3	The organization employs separate development, testing, and production environments for all applications.
	CM-4	The organization has developed and established defined application change management standards and procedures that includes:- Change control/change management software used- Testing/approval requirements- Change status tracking and approval- Emergency change procedures
Application Management (AP)	AP-1	The organization has a process in place to manage critical application access including: - Applications access outside of the network - Management of account administration and the access security process (i.e. password settings, role based access) for the systems - Periodic recertification of user access to applications - Standards and guidelines for the use of generic or shared accounts - Segregation of duties determined/enforced for critical applications - Account misuse controls (i.e. logging, alerts, etc.) in place to help identify either a rogue employee or attacker misusing credentials
	AP-2	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
	AP-3	The organization reviews the information system, on a periodic basis to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and disables functions, ports, protocols, and services within the information system that are deemed to be unnecessary and/or nonsecure.
	AP-4	The organization separates duties of individuals; documents separation of duties of individuals; and defines information system access authorizations to support separation of duties.
	AP-5	The organization performs information system audits that review misuse of privileged functions.
	AP-6	The organization only permits the use of shared/group accounts that meet the organization-defined conditions for establishing shared/group accounts.
Computer Operations (CO)	CO-1	The organization conducts backups of user-level and system-level and system level information contained in the information system based on the predefined recovery time objective and recovery point objective.

	CO-2	The organization tests backup information periodically to verify media reliability and information integrity.
	CO-3	The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.
Response Planning (RP)	RP-1	The organization had developed, established, and updates on a periodic basis continuity of operations documents including Business Continuity and Disaster Recovery Plans.
	RP-2	The organization defines within the continuity of operations documents details to continue mission critical functions such as:- Alternate relocation site- Business impact analysis- Recovery time objectives- Recovery point objectives
	RP-3	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
	RP-4	The organization tests the incident response capability for the information system, on a parodic basis using organization-defined tests to determine the incident response effectiveness and documents the results.
	RP-5	The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
Risk Assessment (RA)	RA-1	The organization develops, documents, and disseminates, to the appropriate personnel, a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
	RA-2	The organization reviews and updates the current risk assessment policy and procedures on a parodic basis.
	RA-3	The organization conducts, documents, reviews, and disseminates results of an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits on an annual basis.

	RA-4	The organization updates the risk assessment, on an annual basis or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
	RA-5	The organization scans for vulnerabilities in the information system and hosted applications on a periodic basis and when new vulnerabilities potentially affecting the system/applications are identified and reported techniques to remove the vulnerability are employed.
	RA-6	The organization tracks and reports information system vulnerabilities associated with reported security incidents to the information security team.