Montgomery County, Maryland

Office of the County Executive

Office of Internal Audit

Information Technology Audit: Change Management

December 11, 2020

MCIA-21-2

Highlights

Why MCIA Did this Review

The Montgomery County Office of Internal Audit (MCIA) conducted an Information Technology (IT) audit of change management processes within selected departments of Montgomery County. The County's IT functions are both centralized and de-centralized. Therefore, each department reviewed has unique change management responsibilities with varying amounts of assistance from the Department of Technology Services (DTS). The audit assessed departmental policies and procedures surrounding the change management process, documented baseline configurations, maturity of the change management process, security impact analysis, and access restrictions for executing changes to critical systems.

This audit was conducted as a result of MCIA's 2019 IT Risk Assessment (ITRA). The focus was to evaluate the current internal control environment of the County's change management process. The audit was conducted by the accounting firm SC&H Group, Inc., under contract with MCIA.

MCIA has identified four findings to strengthen the existing control environment within the County's change management process.

December 2020

IT Audit of the Change Management Process

What MCIA Found

The audit of the County's change management processes identified several opportunities to mitigate risks. The risks can be addressed by enhancing or implementing internal controls within the change management processes.

We identified four findings to strengthen controls and mitigate risks within the enterprise and selected departments' change management processes, including:

1. Developing and/or enhancing detailed procedural documents
2. Implementing a quality assurance process to ensure change management requirements are being achieved
3. Developing configuration baseline and checklist documents
4. Implementing periodic user access reviews of administrative access

TABLE OF CONTENTS

Objectives

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

The audit included meeting with IT personnel from selected departments[1] to build upon the knowledge obtained through the County's ITRA, and to understand the following specific to each selected department:

1. Change management processes responsibilities between the department and DTS
2. Documented policies, procedures, standards, and/or guidelines
3. The number of critical systems used within the department
4. Frequency of changes to critical systems
5. How changes to critical information systems are managed and tracked

The audit's objective was to evaluate the efficiency and effectiveness of the County's internal controls for change management including identification, assessment, verification, and management of changes at the server and application level. Server changes consist of configuration changes made at the server level. Examples include configuring which ports are open or closed, encryption schemes, and available server level services (e.g., file sharing, print resources). Application level changes include but are not limited to changes to the code, functionality, and appearance of the system on the application level.

Background

County-wide Information Technology Overview

The County manages the use of hardware, software, and 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, and increase productivity.

Centralized IT Functions

DTS provides certain IT and communication services necessary to support the daily operation of County departments through seven divisions, offices, and programs:

1. Office of Broadband Programs (OBP)
2. Office of the Chief Information Officer (CIO)
3. Office of the Chief Operating Officer (COO)
4. Enterprise Applications and Solutions Division (EASD)
5. Enterprise Systems and Operations Division (ESOD)
6. Enterprise Telecommunications Services Division (ETSD)
7. Enterprise Resource Planning Division (ERPD)

DTS is responsible for assisting County's departments with the following:

1. Hosting servers.
2. Processing and conducting agreed-upon changes to systems and applications.
3. Providing overall policy guidance and requirements that should be followed by each department when performing a change to critical systems.

[1] "Selected departments" refer to the departments evaluated during the audit. Due to the sensitivity of information provided by departments, and to keep departmental information anonymous, department names are not provided in this public report.

Decentralized IT Functions

Each individual department within the County functions as an IT entity providing evaluation and implementation of advanced data, applications, teleprocessing, and radio systems. Department-specific IT teams are responsible for identifying and managing these advanced approaches for the ongoing operation of Montgomery County departments.

Change Management Overview

Change management is the process and supporting activities to implement software changes from initiation through post implementation monitoring. Appropriately established change management processes and controls provide a consistent and efficient approach to implementing changes to systems and applications. Failure to follow sufficient processes and controls increases the chances of an unsuccessful or poorly managed change, increased time to perform a change, and/or unauthorized changes being pushed into production. Further, these risks could increase the likelihood of a security lapse within critical information systems, including breaches to sensitive information, unauthorized access and successful attacks to sensitive information, and denial of service attacks. The key activities within each change management process includes:

1. Capture Request: Change request should be captured in a centralized location using a standardized form. Items within this form should include, but not be limited to the change description; justification for the change; potential policy impacts; communication of receipt of change request; and periodic communication through each phase of the change.
2. Risk Analysis and Approval: Identifying and documenting the impact a potential change may have on the current IT environment and business processes and the associated likelihood of that impact occurring. This process involves a team of approvers representing both the business and IT stakeholders. Approvals and outcome of the analysis should be documented, including the name of the authorized approver, title of approver, date of approval, and outcome of analysis.
3. Implementation of Request: Once the change has been approved based on the risk analysis, the change should be developed in a non-production environment (e.g., testing or development environment) to ensure the change functions as intended. Required approvals should be solicited from appropriate stakeholders prior to proceeding to implementing the change into production. Implementing the change into production should be coordinated between business and IT stakeholders including agreeing upon an appropriate date and time for implementation. After stakeholders confirm the change is functioning as intended, post implementation approval should be obtained from the stakeholder. Stakeholders and the project manager should update project documents as needed (e.g., change log, affected policies, lessons learned) and develop any necessary training and communication of the change.

Change Management Processes

Most of the departments reviewed as part of this audit had unique critical systems (e.g., financial systems, traffic monitoring systems), varying levels of reliance on DTS, and access to different change management processes and tools (e.g., ticketing systems, excel spreadsheets). Examples of departmental change management processes include the following, from least amount of departmental involvement to a heavy reliance on departmental involvement:

1. The department works solely with a third-party provider to administer all changes to their critical information system.
2. The departmental IT support identifies a need for a change, but works with DTS to execute the change to the system.
3. The department owns all aspects of the change including identifying the need for a change, monitoring and tracking the change using a ticketing system, developing the change, testing the change, executing the change, and monitoring the system post-change for issues.

Scope and Methodology

The audit was conducted from April 2020 to August 2020. The audit focused on the following:

1. Current change management control environment
2. Changes that were completed between May 2019 to May 2020
3. An analysis of the following processes within change management for each selected department:
    a. Established policies and procedures
    b. Documented baseline configurations
    c. Maturity of the process
    d. Security impact analysis
    e. Access restrictions for change

In order to achieve the objectives, SC&H performed the following:

Interviews

Interviews and walkthroughs were conducted with selected departments' IT management and staff involved in the change management process to document internal controls and identify risks associated with each of the following change manage process areas:

1. Governance
2. Change Management
3. Risk Analysis
4. Access Management
5. Configuration Management
6. System Inventory
7. Usage Restriction

Policy and Procedure Review

SC&H reviewed County-wide and selected departmental change management policies and procedures at the server and application level to gain an understanding of current state documented practices and requirements.

Test Plan Development

Utilizing the information obtained during scoping and preliminary department assessment, interview, and walkthrough procedures, SC&H developed an audit plan to test the operational effectiveness of internal controls.

Fieldwork

Fieldwork consisted of testing the operational effectiveness of internal controls identified during scoping and preliminary department assessment, interviews, and walkthrough procedures. SC&H obtained and reviewed documentation needed to satisfy the testing steps developed in the test plan, including populations needed to select samples for which additional information was requested.

Appendix A is provided as reference for all controls tested as part of the audit.

Findings and Recommendations

The following four findings are a compilation of observations identified during the review and are not necessarily applicable to each of the departments reviewed during this audit. These findings were identified to strengthen and expand departmental change management processes and controls.

Due to the sensitive nature of the specific department findings, detailed information is not included in this report. Each department included in this review has received detailed findings and recommendations for review and response. Specific recommendations have been developed to address each department-specific finding; and each department will be required to develop corrective action plans to timely and fully address the recommendations. DTS will be responsible for developing an overall corrective action plan to address the four findings that follow.

1. **Change Management Policies and Procedures**
   Sufficient change management policies and procedures reflective of the current process and control environment have not been developed and/or formalized.

   Failure to document the required procedures related to the change management process could result in a security lapse within critical information systems. This could further result in breaches to sensitive information. Additionally, systems that are not properly configured could result in unauthorized access and successful attacks to sensitive information including, but not limited to, denial of services attacks, ransomware attacks, manipulation of data, and fraudulent activities that can be associated with fines and penalties.

2. **Compliance with Change Management Processes**
   Processes and procedures are not in place to ensure compliance with the change management policies.

   Failure to establish and follow a consistent process for configuration changes to production systems could expose the department and/or the County to vulnerabilities such as unauthorized access to data, manipulation of data, and/or denial of service attacks.

3. **System Configuration Checklist and Baseline Configurations**
   System configuration checklist and baseline configurations have not been developed and/or formalized.

   Systems that are not properly configured for security could result in unauthorized access and successful attacks to sensitive information including, but not limited to, denial of services attacks, ransomware attacks, manipulation of data, and fraudulent activities that can be associated with fines and penalties. Additionally, failure to document the required standard security related configuration settings could result in a security lapse when changes are conducted within critical information systems. This could further result in breaches to sensitive information.

4. **Administrative Access Management**
   Periodic user access reviews are not being conducted on a consistent basis to monitor administrative accounts and ensure appropriate access to critical applications.

   Inappropriate users having elevated access to critical information systems could expose the department and/or the County to vulnerabilities such as unauthorized access to data, manipulation of data, and/or denial of service attacks. Additionally, inappropriate users having configuration access to critical information systems may expose the department and/or the County to unauthorized changes, data leakage, and fines associated with national and federal standards and regulations.

Comments and MCIA Evaluation

We provided the Department of Technology Services (DTS) with a draft of this report for review and comment. DTS responded with comments on December 7, 2020, and the response has been incorporated in the report at Appendix B. DTS concurred with the findings identified in the report, indicating that the department has taken steps to address some of the findings, specifically to advance change management, deployment, and configuration management accountability. Additional steps will be supported with the implementation of the DTS reorganization. No changes have been made in the report based on the response.

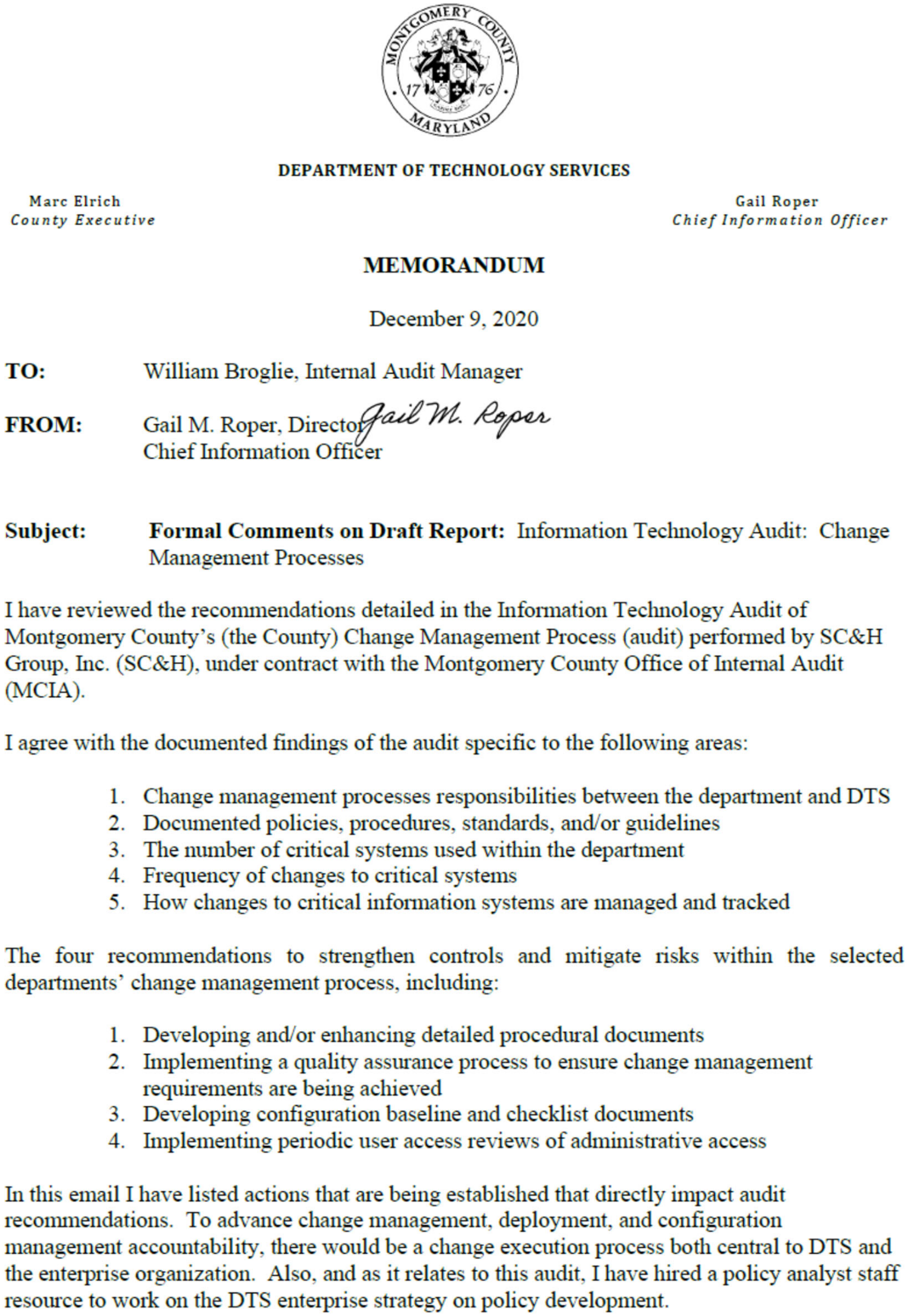
Appendix A – Areas of Focus

Domain	Control #	Control Description
Governance	CM-1	The organization: a. Develops, documents, and disseminates to the appropriate County and/or departmental personnel or roles: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy based on the County and/or departmental defined frequency; and 2. Configuration management procedures based on the County and/or departmental defined frequency.
	CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
	CM-9	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.
Change Management	CM-3	a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system;

Domain	Control #	Control Description
		d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for the County and/or departmental defined time period; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through the County and/or departmental defined configuration change control element (e.g., committee, board) that convenes based on the County and/or departmental defined frequency; and/or the County and/or departmental defined configuration change conditions.
Risk Analysis	CM-4	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
Access Management	CM-5	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
	CM-7	a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: based on the County and/or departmental defined prohibited or restricted functions, ports, protocols, and/or services.
Configuration Management	CM-6	The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using the County and/or departmental defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for the County and/or departmental defined information system components based on the County and/or departmental defined operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
	SA-10	The organization requires the developer of the information system, system component, or information system service to:

Domain	Control #	Control Description
		a. Perform configuration management during system, component; or service design, development, implementation, and/or operation; b. Document, manage, and control the integrity of changes to the County and/or departmental defined configuration items under configuration management; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to the County and/or departmental defined personnel.
Inventory	CM-8	The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory based on the County and/or departmental defined frequency.
Usage Restrictions	CM-11	The County and/or department: a. Establishes policies governing the installation of software by users; b. Enforces software installation policies through the County and/or departmental defined methods; and c. Monitors policy compliance at the County and/or departmental defined frequency.

Appendix B - DTS Response



DEPARTMENT OF TECHNOLOGY SERVICES

Marc Elrich
County Executive

Gail Roper
Chief Information Officer

MEMORANDUM

December 9, 2020

TO: William Broglie, Internal Audit Manager

FROM: Gail M. Roper, Director Gail M. Roper
Chief Information Officer

Subject: **Formal Comments on Draft Report:** Information Technology Audit: Change Management Processes

I have reviewed the recommendations detailed in the Information Technology Audit of Montgomery County's (the County) Change Management Process (audit) performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County Office of Internal Audit (MCIA).

I agree with the documented findings of the audit specific to the following areas:

1. Change management processes responsibilities between the department and DTS
2. Documented policies, procedures, standards, and/or guidelines
3. The number of critical systems used within the department
4. Frequency of changes to critical systems
5. How changes to critical information systems are managed and tracked

The four recommendations to strengthen controls and mitigate risks within the selected departments' change management process, including:

1. Developing and/or enhancing detailed procedural documents
2. Implementing a quality assurance process to ensure change management requirements are being achieved
3. Developing configuration baseline and checklist documents
4. Implementing periodic user access reviews of administrative access

In this email I have listed actions that are being established that directly impact audit recommendations. To advance change management, deployment, and configuration management accountability, there would be a change execution process both central to DTS and the enterprise organization. Also, and as it relates to this audit, I have hired a policy analyst staff resource to work on the DTS enterprise strategy on policy development.

The standardization of change execution requires strategy, process, and resources. The original structure of the DTS organization did not support or leverage the development of a risk rating scale that identifies an agile approach to evaluate or standardize change requests. This was acknowledged and incorporated into the DTS reorganization.

The DTS Organizational Restructure:

The Department of Technology Services has been reorganized. The reorganization was submitted with the FY21 Budget and should be in effect in January 2021. After much consideration, a modern organizational structure that supports the development of an IT Organizational Framework is being adopted. This report details centralized vs. decentralized efforts of change management. The audit supports the issue of a lack of established change management processes and policy. The DTS organization can be positioned to enhance those organizations that it supports. The change management practice is underdeveloped in the DTS organization. For DTS to influence or model best practice change management the following organizational structures and resources have been established.

The new Organizational Framework for DTS:

- The involvement of DTS in decentralized agreements, including cloud deployment activities will be done in partnership with DTS.
- The Office of the CIO has developed a division, Office of Strategic Partnerships, which will work closely with establishing and partnering with departments. This division will house the policy analyst and policy development.
- The Office of Digital Transformation will focus on digital transformation, low-code, no-code development including the necessary establishment of a risk rating scale and change, release, and deployment workflow.
- The Office of Project Management will provide oversight on the PMO maturity model for IT projects including system innovation, risk management, and executive oversight.
- The Office of Enterprise Information Security oversees the risks and security efforts associated with system changes. The Varonis tool is a discovery tool that has been purchased to operationalize audit capabilities to identify and monitor administrative accounts and ensure appropriate access to critical information systems.
- The One Face Forward Initiative leads the new Change Control Board (CCB). The review of the Service Now service tool for change management is being considered as an enterprise change management solution. This would provide a Change Management Data Base and workflow tool. The CCB was established to define change management efforts for the 0365-infrastructure including establishing a model that can be expanded to enterprise system changes. The CCB will establish monthly and quarterly schedules for the review of change requests including decision support to effectively speed and establish accuracy of the organizational change process.
- The Office of Change Management will enhance all aspects of change management including business process reengineering efforts.

Current State Strategies in Progress:

- Formal change management is in the very early adoption stage with the DTS organization.
- The change management effort is focused on the ability to identify and initiate change requests, evaluate change, coordinate change, execute change, and review change.
- Change management is a cultural practice and is not highly recognized and implemented by most IT organizations within Montgomery County making it challenging to establish organizational change management directives and practices.
- Our plans for the implementation of digital business initiatives identify the change management culture as a significant roadblock.
- There is a strategy element to implement best practices for the office of change management and change leadership. DTS will select approaches that align with the organization's culture to ensure shared understanding, a common approach, and consistency in practice execution.
- We are working towards building organizational change management capabilities by adopting an enterprise approach based on established industry best practices and integrating those practices into program and project planning.
- DTS is fostering change leadership capabilities within the IT management team by communicating, practicing, and reinforcing change leadership practices using a recognized model to develop a resilient organization ready and able to respond to digital business and business continuity.