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

Information Technology Audit
Access Management

February 9, 2022

MCIA-22-1

Highlights

Why MCIA Did this Review

The Montgomery County Office of Internal Audit (MCIA) conducted an Information Technology (IT) audit of access management processes within selected departments of Montgomery County and divisions within the Department of Technology and Enterprise Business Solutions (TEBS). The County's IT functions are both centralized and de-centralized. Therefore, each department reviewed has unique access management responsibilities with varying amounts of assistance from TEBS. The audit assessed departmental policies and procedures surrounding access management and authentication management process, the process of authorizing and managing logical access to systems for County employees and non-County employees (e.g., volunteers, interns, contractors, and vendors), and processes and performance of background checks. Additionally, the audit reviewed the process for ensuring appropriate roles are granted, the process for adjusting access in the case of interdepartmental and intradepartmental staff transfers, and the access termination process.

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

FEBRUARY 2022

IT Audit of the County's Access Management Processes

What MCIA Found

The IT audit of the County's access management processes determined that established IT access management processes and controls reduce the risk of inappropriate access to systems, applications, and data; minimize segregation of duties conflicts; and secure access to critical and sensitive data. The audit identified seven recommendations to strengthen controls and mitigate risks within the County's IT access management processes.

1. Require annual review of access management policies and procedures.
2. Implement processes to ensure new access request forms are easily accessible, provide sufficient detail regarding access requested, include appropriate authorization and approval of access, and ensure roles requested follow the "least privilege needed" principle.
3. Ensure authentication guidelines implemented meet the Information Security System and Data Owners Handbook requirements.
4. Implement processes to document all required service accounts and restrict access to service accounts to only critical users.
5. Update the current language utilized as the background check policy and create risk designations.
6. Implement processes to ensure that Organization Unit (OU) transfers are requested by the department and processed in a timely manner.
7. Implement processes to ensure that access requests associated with termination notices are processed within 24 hours of receipt of the notice.

TABLE OF CONTENTS

Objectives

This report summarizes the information technology (IT) audit of Montgomery County's (the County) access management processes (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 selected divisions within the County's Department of Technology and Enterprise Business Solutions (TEBS) and selected departments to build upon the knowledge obtained through the County's IT Risk Assessment conducted in 2019, and to understand the following specific tasks regarding access management:

1. Documented policies, procedures, standards, and/or guidelines regarding access and authentication to critical systems
2. IT access management responsibilities
3. Background check policies and practices regarding access management
4. Processes for access requests, authorization, and role assignment
5. Processes regarding interdepartmental and intradepartmental staff transfers
6. Processes regarding access termination

The audit's objectives were to:

1. Ensure that the appropriate access control policies and procedures have been established, reviewed, and updated on a periodic basis.
2. Ensure that the access management process is controlled, monitored, and reviewed in compliance with industry best practices.
3. Ensure that all access requests are processed in a controlled manner including standard and administrative access to critical systems and supporting components (e.g., servers and databases).
4. Ensure that there are effective controls in place to provide appropriate separation of duties, including defining and documenting specific duties of individuals/positions that are to be separated and ensure appropriate enforcement of the separation.
5. Ensure that appropriate log-in controls are in place for critical systems, system components, and networks.

Background

County-wide Information Technology Overview

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

TEBS is responsible for assisting the County's departments with identifying innovative technology solutions, helpdesk support, IT security, IT asset procurement and management, and access management for Active Directory (AD) and Oracle Enterprise Resource Planning (ERP). AD is a directory service for Windows domain networks. Oracle ERP manages enterprise functions including accounting, financial management, project management, and procurement.

IT Access Management Overview

IT access management is the overall process of requesting, approving, updating, monitoring, and removing access to systems and applications across the organization. This includes components of the new hire process, such as conducting background checks in accordance with policy, automated processes to streamline the creation and termination of user accounts, and authentication policies and procedures for accessing systems. Established IT access management processes and controls reduce the risk of inappropriate access to systems, applications, and data; minimize segregation of duties conflicts; and secure access to critical and sensitive data. Failure to follow sufficient processes and controls could result in inappropriate access, which could expose the County to vulnerabilities such as unauthorized access to data, manipulation of data, and/or denial of service attacks.

Centralized IT Access Management Functions

TEBS provides IT access management services and support through the following offices and divisions within those offices:

1. Office of Broadband Programs & Infrastructure Modernization
2. Office of Digital Transformation
    a. Infrastructure and Cloud Services
    b. Enterprise Resource Planning
3. Office of Enterprise Information Security

The offices and divisions referenced above are responsible for assisting the County's departments with the following access management support:

1. Providing overall policy guidance and requirements that should be followed by each department regarding access and authentication management.
2. Processing and creating AD and ERP accounts utilized by all County employees and, as applicable, non-County employees (e.g., volunteers, interns, contractors, and vendors).[1]
3. Processing and updating of all interdepartmental AD Organizational Unit (OU) transfers.
4. Processing and disabling of all termination requests for County employees and, as applicable, non-County employees.

Individual departments are responsible for managing user access to departmental specific applications and access privileges within their respective AD OU.

IT Access Management Processes

The County has implemented specific policies and procedures, and processes/controls to manage access to IT systems and applications, including the following:

1. **Policies and Procedures:** TEBS and the selected departments rely upon Administrative Procedure (AP) 6-7 as the information security policy regarding access and authentication management processes. This includes the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook as appendices to AP 6-7, which provide additional requirements concerning the use of County systems and technology. Within TEBS, there are additional supplementary policy and procedural documents that cover the following areas:
    a. Technical architecture of County systems,
    b. AD and ERP account processes,
    c. Identity management rules,
    d. Multi-factor authentication policy and processes,

[1] Any future reference of "non-County employees" encompasses volunteers, interns, contractors, and vendors unless specifically referenced.

e. Microsoft Office 365 (O365) administrator guidelines, and
f. AD Organizational Unit administrator training manual.

Further, several of the selected departments have additional policies to supplement AP 6-7 and/or to specifically provide detailed access management procedures regarding a critical application to that department; however, all departments utilize AP 6-7 as the foundation of their information security processes and all supplemental policies must comply with AP 6-7.

2. **Account Creation:** As new County employees and non-County employees are onboarded to the County, a background check is required for all public safety personnel (e.g., Police and Fire and Rescue employees, volunteers, and interns), Finance, and Circuit Court employees. Additionally, employees and contractors that require access to federal systems must also undergo a background check. For TEBS employees, only roles with a risk designation requiring additional screening processes are required to have a background check. This risk designation describes the associated risk of certain systems, applications, and IT positions that require a background check. This includes federal system access for employees and contractors, and certain County systems. Once the initial hiring documentation is completed, including a background check if required, the automated AD and Oracle nightly account creation job identifies changes to the user's record in Oracle and creates an account. The user's record can be modified by either the Office of Human Resources (OHR), or the user accepting the position in the recruiting portal of Oracle. Both of these actions automatically update the user's Oracle security record and begin the automated account creation process.

   AP 6-7 includes guidance on granting the least privileged access needed to complete job functions. Least privileged access is the minimum level of access, system and/or network access, that allows a user to carry out tasks associated with their job responsibilities. The user's supervisor may request additional access through various methods (e.g., ServiceNow tickets, email communications, or new hire forms) beyond the standard account created via the iamMCG automated process, the County's access management provisioning solution that is managed by TEBS. The supervisor will communicate to the appropriate administrator of that application or system for additional access. This formal request from an appropriate supervisor is the authorization and approval required for additional access. After approval has been obtained, the administrator of the system reviews, within reason (e.g., administrative roles for non-IT staff would not be granted or accounting roles for non-accounting staff, etc.), the roles being requested and confirms they are appropriate based on the user's job and/or responsibilities.

3. **Authentication:** User authentication guidelines are documented in AP 6-7, including the use of multi-factor authentication (MFA), minimum parameters for passwords, account lockout attempts, and account lockout durations. To gain access to the County's network, MFA was implemented as a requirement of use for all users' login as of July 15, 2021 and for all users accessing the network via virtual private network (VPN) on July 12, 2021. Additionally, all users are assigned unique user identification and password credentials for systems access, including administrative users who are assigned a Gen-account (i.e., Gen-"Username", generic-account for administrative use), in addition to their standard account (i.e., "Username"). All administrative activities are completed using their Gen-account; whereas, non-administrative tasks are completed using their standard account.

4. **Account Transfers:** The County frequently has staff transferring from one department to another, or transferring within a department (interdepartmental and intradepartmental transfers, respectively). Each department has an individual departmental organizational unit (OU). An OU is a department sub-directory within AD domain that allows administrators to group users and computers together to assign policy settings and/or account permission. This function allows administrators to manage the day-to-day administrative responsibilities of the department; however, those administrators are limited to responsibilities within their department. The TEBS-Active Directory (TEBS-AD) group is responsible for transferring a user between OUs upon receipt of a request from the new department requesting the transferred user be moved into the new OU. ERP roles are automatically stripped for users moving to new departments once HR updates the respective Oracle security record to the new department designation. Access to other applications is modified as needed, as some users may have transitional work for their former department that must be completed after their initial transfer date. Intradepartmental transfers have access changes requested as needed, but there is no formal policy or procedure regarding user access for intradepartmental transfers.

5. **Account Termination:** Similar to the account creation process described above, account terminations for AD and Oracle ERP are terminated through the daily iamMCG automated process following the department's HR liaison entering the termination details directly into the respective user's security record. Daily, the iamMCG automated job runs, and that identifies all users whose security record has been modified to include the termination assignment and disables their AD and Oracle ERP accounts. Additional access to applications and systems that are not authenticated through AD require a formal request submitted (e.g., ServiceNow tickets, email communications, or termination forms) to the administrators of those applications for access removal.

6. **Application Logging:** The County has implemented multiple means of monitoring user access at the application level and a variety of methods are utilized to create logs for access and usage, including the following:
   a. The County has multiple scripts that look for and track unusual behaviors (e.g., accessing several documents in a brief time within O365 or requesting access multiple times and being denied).
   b. The County has activity logs enabled and maintained to track user access for the following areas:
      i. AD
      ii. DataNET Hub Secure Transfer Protocol (DNHSTP) - secure version of file transfer protocol
      iii. Anti-virus (Windows Defender) - computer program used to prevent, detect, and remove malware
      iv. Network Switch - connects devices on a computer network by using packet switching to receive and forward data to the destination device
   c. Access to core applications are being monitored via Microsoft Sentinel (scalable, cloud-native, security information event management (SIEM) solution), which was implemented at the County in the past two to three years. There are approximately 300 applications being monitored through this and more are being added as they go through the integration process. Some of the key County systems that are being monitored include ERP, O365, HR management system, and 911 system/CAD. Log reviews occur based on the incident response

playbook (i.e., if an incident occurs, TEBS follows the processes outlined in the playbook).

Scope and Methodology

The audit was conducted from June 2021 to September 2021. The audit focused on the current IT access management processes maintained and administered by selected divisions within TEBS and selected departments within the County. Processes included the following:

1. Access control policies and procedures, content, and document development to ensure access control functions are performed in a standardized manner for County employees, vendors, and contractors.
2. Access management processes and supporting activities necessary to appropriately manage user access to applications, information systems, and information system components for County employees, vendors, and contractors.
3. Process of requesting, authorizing, monitoring, and reviewing access to applications, information systems, and information system components for County employees, vendors, and contractors.
4. Process and performance of background checks and user access entitlement reviews (recurring review of access rights, or permissions) for County employees, vendors, and contractors.
5. Access management tasks to ensure appropriate segregation of duties for roles and responsibilities.
6. Log-in process in place for applications, information systems, and information system components.

The audit also included an analysis of the following aspects related to the IT access management processes:

1. Maturity of the process,
2. Number of critical systems,
3. Ownership of the various functions within the process, and
4. Applicable NIST 800-53 rev. 4 controls.[2]

Scope criteria included IT access activity that occurred within the period of June 1, 2020 to June 1, 2021.

Scoping

SC&H performed the following procedures to obtain a preliminary understanding of the County's IT access management functions.

Interviews

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

1. Governance
2. Account Management
3. Account Identification and Authentication

[2] Security and Privacy Controls for Federal Information Systems and Organizations: https://nvd.nist.gov/800-53/Rev4. Issued by the non-regulatory agency of the United States Department of Commerce, NIST 800-53 contains a catalog of security and privacy controls for all U.S. Federal Information Systems except those related to national security. This standard contains best practices as a guideline for IT security and privacy controls.

4. Personnel Screening
5. Terminated Users
6. Transferred Users

Policy and Procedure Review

SC&H obtained and reviewed access and authentication management policies and procedures from the selected divisions of TEBS and selected departments.

Test Plan Development

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

Fieldwork

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

Scope Limitations

As noted in the previously issued IT Vendor and Contractor Management Internal Audit Report, there is no periodic review of non-County employee IT access in place to ensure IT access is appropriate and/or removed in a timely manner.[3] This finding is under remediation; therefore, non-County employees were not sampled as part of the terminated user sample.

Sample Selection

Access samples were separately selected based on the respective size of the population identified.

New Hire – County Employees

SC&H selected 40 samples from a total population of 302 newly hired employees. In order to sample from the sub-population (i.e., departments) in a more representative nature, the population was subdivided into selected departments and then samples were randomly selected based on their proportion to the total population.

Newly Onboarded – Non-County Employees

SC&H selected 25 samples from a total population of 375 non-County employees. The samples were judgmentally selected based on their proportion to the population of TEBS or selected departments.

Transferred Employees

SC&H selected 20 samples from a total population of 72 transferred employees. The samples were judgmentally selected based on their proportion to the population of TEBS or selected departments. The sample included 10 intradepartmental transfers and 10 interdepartmental transfers.

[3] See finding 2 of the IT Vendor Contractor Management Report for additional detail, risks associated, and recommendations. https://www.montgomerycountymd.gov/exec/Resources/Files/audit/IT_Vendor_Contractor-6-2021.pdf

Terminated Employees
SC&H selected 25 samples from a total population of 294 terminated employees. The samples were judgmentally selected based on their proportion to the population of TEBS or selected departments.

Documentation Review
SC&H obtained and reviewed AP 6-7, including the Information Security System and Data Owners Handbook, which is the County's established policies and procedures for compliance with information security policy in the use of the County's technological devices. AP 6-7 includes, but is not limited to the following areas related to access and authentication management:

1. Information System Access Control
2. Information Security Assessments and Privacy Assessments, Authorization, and Monitoring
3. Identification and Authentication
4. Personnel Security

Walkthroughs
Walkthroughs were performed with the selected divisions of TEBS and selected departments to obtain a more thorough understanding of each sub-process to evaluate the effectiveness of internal controls, the workflow between TEBS and the selected departments, and the division of access management responsibilities.

Internal Controls Testing
Internal controls identified and detailed within the audit plan were tested to assess the operating effectiveness of the identified control activity. SC&H prepared a document request list for all support needed to satisfy the testing steps and associated attributes detailed within the audit plan.

1. New Hire – County Employee: For each sample selected, SC&H obtained supporting documentation to validate the request for access, the approval of access prior to access being provisioned, and if the access provided appeared reasonable based on the user's job title and responsibilities.
2. Newly Onboarded – Non-County Employee: For each sample selected, SC&H obtained supporting documentation to validate the request to create the non-County Employees AD account and to ensure that the request was completed prior to their account being created.
3. Transferred Employees: For each sample selected, SC&H obtained supporting documentation to validate the user had an OU transfer completed, if applicable for their transfer, and evidence that roles were adjusted based on documented requests.
4. Terminated Employees: For each sample selected, SC&H obtained supporting documentation to validate the notification of termination, user listings to confirm that access was removed for terminated users, and evidence of their Oracle ERP account being disabled via the automated process.

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

Findings and Recommendations

The following seven findings' categories and recommendations are a compilation of observations identified during the audit. Individual findings apply specifically to those departments or divisions named within each finding below. These findings were identified to strengthen and expand departmental access management processes and controls.

Due to the sensitive nature of the specific department findings, certain detailed information is not included in this report. Any detailed or technical information deemed sensitive has been communicated directly with the responsible department. 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. TEBS will be responsible for developing an overall corrective action plan to address the findings and recommendations that follow.

1. **Access Management Policies and Procedures**

   The intent of IT access management policies and procedures are to provide guidance and procedures to perform specific actions within the access management process. It is important that policies are reviewed at least on an annual basis to confirm that the current process and control environment are accurately reflected within the respective policy. AP 6-7, Section 4.2.3, states that departments are responsible for reviewing and updating department-specific information security policies and procedures annually. This audit identified policies that are either outdated and/or infrequently reviewed in the following divisions and/or departments:

   1.1 TEBS-AD

   The following IT access management policies did not have formal evidence of a documented review within the last year.

   1. Enterprise Architecture Technical Architecture
   2. Automated AD and Oracle Account Provision Process for Employees
   3. Departmental OU Training Manual

   1.2 Police Department (MCPD)

   The following IT access management policies did not have evidence of a documented review within the last year.

   1. Department Information Systems
   2. Internet, Intranet, and E-Mail Operations
   3. Career Enhancement System (Training)
   4. Written Directive System (Creation of SOPs)
   5. Standard Operating Procedures (Security Annex 4)
   6. MCP Web Board

   Risks

   1. Failure to review and document the required procedures related to the IT access management process could result in security lapses and/or breaches to sensitive data within critical information systems.
   2. Outdated IT access management policies and procedures 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.[4]

Recommendation 1.1
TEBS-AD and MCPD should review access policy documentation at least annually, in accordance with AP 6-7, Section 4.2.3, and whenever known changes are made to the policies to ensure that all processes, procedures, and practices are still in use, effective, and efficient to operate as needed in the County's current technology environment. Any changes identified should be reviewed, approved, and incorporated into the policy documentation in a timely manner and communicated to all appropriate stakeholders.

Recommendation 1.2
Once all policy documentation is updated based on Recommendation 1.1, TEBS-AD and MCPD should communicate and/or conduct an internal training to ensure all parties are aware of changes to existing and new policies, procedures, and processes.

2. New Access Requests

New user access requests serve as the initial process for documenting the request, authorization, and approval for access that users are granted within the County's information systems. Evidence of access requests should be accessible to relevant users, provide details regarding the access being granted, show evidence of authorization and approval of access prior to access being provisioned, and follow the principle of least privilege, providing only the access needed to complete a user's job roles and responsibilities. This audit identified various findings in the new access provisioning processes within the following in scope divisions and/or departments:

2.1 Circuit Court (CCT)
For one out of three samples, elevated access privileges were granted beyond the user's job responsibilities. SC&H confirmed through inquiry that the sampled user had been assigned additional access as part of their previous state court employment and that elevated access privileges remained during their transition to a County court employee. Additional details regarding the identified user are included in separate communication directly with CCT.

2.2 TEBS-AD
For four out of 40 samples, documentation supporting authorization and approval of access prior to access provisioning was not available. The four sampled accounts were initially created prior to the iamMCG automated process that was implemented in 2019, and these users were re-hired by the County within SC&H's testing period. These accounts had to be manually activated and connected to their original accounts versus being created through the automated process. As a result, documentation was not available supporting the re-activation of these accounts to validate appropriate authorization and approval.

2.3 Department of Health and Human Services (HHS)
For 11 out of 15 samples, documentation supporting the request, authorization, approval of access prior to access provisioning, and access provisioned based on job responsibilities was not provided.

[4] Fines and/or penalties can arise from non-compliance with laws and regulations (e.g., Health Insurance Portability and Accountability Act (HIPAA) of 1996, Homeland Security Act, which included the Federal Information Security Management Act (FISMA) of 2002, or the Cybersecurity Information Sharing Act (CISA) of 2015).

2.4 MCPD
For nine of the nine samples selected, documentation supporting the request, authorization, approval of access prior to access provisioning, background check, and access provisioned based on job responsibilities was not provided.

Risks

1. Failure to retain or show evidence of authorization and approval could result in inappropriate users having access to critical information systems.
2. Inappropriate users having access to critical information systems may expose the department and/or the County to unauthorized changes, data leakage, and fines associated with federal standards and regulations.[4]
3. Inappropriate users having access to accounts 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.

Recommendation 2.1
CCT should ensure that employees address any access questions that arise during the access provisioning process with their supervisor and/or the user's supervisor to ensure that access is appropriate and follows the least privileged access principle. Resolutions to address questions should be formally documented in the access request ticket.

Recommendation 2.2
CCT should consider mirroring a user's access based on similar job descriptions to consistently apply access across the department. Ensure initially mirroring of users is reviewed to follow least privileged access principle.

Recommendation 2.3
TEBS-AD should retain and save requests to manually linked accounts when they encounter employees being re-hired to the County from a period prior to the implementation of the current iamMCG automated process.

Recommendation 2.4
HHS and MCPD should implement processes to maintain all new hire access requests including, but not limited to the notifications from OHR, requests, authorizations, evidence of a background check, and approvals of access requested.

3. Authentication Parameters

Authentication parameters set the security foundation for access to County information systems. This audit identified issues regarding the authentication parameters and guidelines in the following divisions and/or departments:

3.1 TEBS-AD
In reviewing AP 6-7, with the county-wide authentication settings for AD, SC&H identified the following area of noncompliance with the authentication parameters provided: Lockout policy.

Additional details regarding the noncompliance are included in separate communication directly with TEBS-AD.

3.2 MCPD
Documentation supporting the authentication parameters was not provided for two of the four in-scope applications.

Risk

Applications and systems not configured to the minimum standard of the County's information security policies and procedures could expose the County to data disruptions, security threats, and/or data breaches.

Recommendation 3.1
TEBS-AD should update all critical information systems' authentication settings to be in compliance with the documented County information security policies and procedures.

If any critical information systems settings or parameters cannot be in compliance to the extent documented in information security policies, an exception document should provide details as to why the system cannot be set to the policy standard, along with approval from the system's business owner and system's support team.

Recommendation 3.2
MCPD should implement processes to ensure the authentication parameters are documented and are in compliance with authentication guidelines within AP 6-7.

If any critical information systems settings or parameters cannot be in compliance to the extent documented in information security policies, an exception document should provide details as to why the system cannot be set to the policy standard, along with approval from the system's business owner and system's support team.

4. Service Accounts

Service accounts provide access to applications to perform maintenance and/or accounts to be utilized by the developer of the application. This audit identified various issues regarding access provisioning of service accounts in the following departments:

4.1 Department of Fire and Rescue (FRS)
SC&H identified the use of generic service accounts within a critical FRS application. Additional details regarding the use of generic service accounts are included in separate communication directly with FRS.

4.2 HHS
SC&H identified the use of generic service accounts within certain critical HHS applications. Additional details regarding the use of generic service accounts are included in separate communication directly with HHS.

4.3 MCPD
Documentation supporting access, including generic service accounts, administrative accounts, and standard accounts, to the in-scope applications was not provided for three out of four of in-scope applications.

Risks

1. Failure to restrict access could result in a security lapse within critical information systems. This could further result in breaches to sensitive information.

2. Failure to restrict access could result in access to critical information systems which may expose the department and/or the County to unauthorized changes, data leakage, and fines associated federal standards and regulations.[4]
3. Inappropriate users having access to accounts 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.

Recommendation 4.1
FRS should continue researching and innovating methods of restricting generic account access to devices, including but not limited to, biometric log on capabilities and other methods of securing the units from inappropriate access.

Recommendation 4.2
HHS should consider restricting generic account access and periodically review the activities completed with these accounts to ensure that activity is limited to only operating the displays within the locations.

Recommendation 4.3
MCPD should implement processes to support generating complete user listings. Access to service accounts should be restricted and periodically reviewed to ensure that activity is limited to only appropriate actions for services accounts.

5. Background Check Policy

Background checks provide reasonable assurance regarding the verification of new hires and newly onboarded users to County information systems. This audit identified the following issue regarding background check policies and procedures in the following division:

5.1 TEBS
TEBS-EIS relies on AP 6-7, Section 13, as the guidance for determining whether a background check is a required component of the hiring process for a position based on a risk designation being assigned to each position. Associated risk designations have been drafted. However, formal background check procedures have not been implemented and associated roles and responsibilities have not been finalized and communicated to appropriate stakeholders.

Risks
Failure to establish and follow a consistent background check process could expose the County to the following possible risks, including, but not limited to:

1. Employees falsifying their credentials for positions;
2. Fraud, hacking and cybercrime, and negligent hiring practices; and
3. Unsafe conditions for customers and employees.

Recommendation 5.1
TEBS should update AP 6-7 to clearly define the screening criteria that will be utilized as part of Section 13 (e.g., credit, criminal, complete background checks, or some combination based on risk designation) to provide sufficient guidance for TEBS and all County departments that utilize AP 6-7 as their primary information technology security policy.

Recommendation 5.2

TEBS should communicate policy updates and/or conduct an internal training to ensure all parties are aware of changes to existing and new policies, procedures, and processes.

6. Transferred Employee Requests

The County has two types of transfer requests: intradepartmental transfers (e.g., promotions, demotions, and title changes) and interdepartmental transfers (i.e., leaving department A to go to department B). Interdepartmental transfers require a department transfer request to transfer AD accounts across OUs. Intradepartmental transfers do not require an OU transfer; however, access changes may be required based on changes in a user's job responsibilities. This audit identified issues regarding the transferred employee request process in the following division and departments:

6.1 TEBS-AD

Based on results of testing, the formal policy requiring a notification to the Help Desk within five (5) days of formal transfer action is not enforced. OU department transfer requests were not requested in a timely manner for two out of 20 samples selected. Additional details regarding the transferred employees OU requests are included in separate communication directly with TEBS-AD.

6.2 Department of Finance (FIN)

Based on the testing performed, a transfer request ticket documenting roles that should have been removed for a transferred employee was created; however, all requested changes associated with that request were not completed for one of three samples selected. Additional details regarding the transferred employee's requests are included in separate communication directly with FIN.

6.3 HHS

Transfer access request tickets were not provided for four of the eight samples selected. Additionally, for two of the remaining four samples no evidence was provided documenting required review of access to determine appropriateness based on the user's new job role and responsibilities.

6.4 MCPD

Transfer access request tickets were not provided for three of the three samples selected.

Risks

1. Failure to remove roles or permissions from transferred employees could result in user's having conflicting, and/or overlapping access to sensitive data.
2. Inappropriate users having access to critical information systems may expose the department and/or the County to unauthorized changes, data leakage, and fines associated with federal standards and regulations.[4]
3. Inappropriate users having access to accounts 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.

Recommendation 6.1

TEBS should enforce processes to ensure OU transfer requests are submitted timely for newly transferred employees. Further, TEBS should communicate these processes throughout the County to ensure that departments are aware of their responsibilities regarding OU transfers.

Recommendation 6.2
Community Engagement Cluster (CEC) should implement and enforce processes to timely submit OU transfer requests for transferred employees. Following, CEC should communicate these processes throughout the County to ensure that departments are aware of their responsibilities regarding OU transfers.

Recommendation 6.3
FIN should ensure that all requested roles are added or removed per the access request tickets, including but not limited to ensuring that access change requests are completed in an accurate and timely manner.

Recommendation 6.5
HHS and MCPD should implement processes to maintain all transfer access requests including, but not limited to the notifications from HR, requests, authorizations, and approvals of access requested.

Recommendation 6.6
HHS and MCPD should implement documented user access reviews for transferred employees to ensure that their roles are appropriate for the job role and responsibilities and do not have conflicting or overlapping permissions.

7. Termination Access Requests

Terminating user access to County information systems is a critical process to ensure the security of County systems and data. There is a combination of automated and manual processes utilized to remove terminated users from County systems. This audit identified issues regarding the access termination requests, notification, and application access cleanup in the following divisions and departments:

7.1 TEBS Enterprise Resource Planning (TEBS-ERP) and Office of Human Resources (OHR)
For nine out of 25 samples selected, termination requests and/or notifications were not entered timely into Oracle, leading to terminated users maintaining access rights beyond their termination date. Termination dates must be entered into Oracle by respective department HR liaisons, approved, and then routed for OHR's final review and approval before the daily automated termination job runs which will identify a user whose status has been modified. While the automated job is designed to ensure access is removed promptly, it relies on the timeliness of manual entries by each department's HR liaison, the approval process within each department, and OHR's approval of the termination documentation. Additional details regarding terminated access requests are included in separate communication directly with TEBS-ERP and OHR.

7.2 FRS
For one out of four samples, termination notification was not communicated to the department HR liaison and management within FRS in a timely manner. The respective email notification was sent out to the department over 24 hours after the employee's resignation from the County.

7.3 HHS
7.3.1. For six out of six samples, termination notifications (e.g., HR notification, Helpdesk ticket, or emails requests) were not provided. Further, the following was noted:

1. For one out of six sampled users, evidence was not available to determine if a termination notification was sent, when the account was disabled, and if the account was disabled within 24 hours per AP 6-7, Section 13.3.1.
2. For one out of six sampled users, evidence was not available supporting termination notification and NextGen access.
3. For two out of six sampled users, access to in-scope critical applications was not removed upon termination. Access to these applications would additionally require users to have physical access to a County laptop and their VPN access, which would have been returned on their last day of employment.

7.3.2. For two in-scope critical applications, there were accounts for users that no longer have Microsoft Outlook accounts (i.e., terminated users). CMT database had 32 terminated users out of 52 users still showing as a user on the user listing. Records Archive (HHS database) had 10 terminated users out of 81 users still showing as a user on the user listing. Access to these accounts would require users to have retained their County laptop and their VPN access, which would have been returned on their last day of employment.

7.4 MCPD
For eight out of eight samples, termination notifications and/or requests for access termination was not provided.

Risks
1. Failure to enter termination requests timely could result in users continuing to have access to County data.
2. Terminated users having 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.
3. Terminated users having access to critical information systems could expose the department and/or the County to unauthorized changes, data leakage, and fines associated federal standards and regulations.[4]

Recommendation 7.1
TEBS should perform an assessment to determine what time frame it feels is appropriate for the manual processes of terminating access to be completed in a timely manner. Based on this assessment, TEBS should consider the following options:
1. Accept that the existing process will have manual delays due to the departments needing to enter, approve, and route the termination to OHR for final approval;
2. Determine that the risk from these delays is too great to accept and work with OHR and departments to determine processes for reducing the time it takes for the departments to enter, approve, and route the termination to OHR for final approval; or
3. Determine that the risk from these delays is too great to accept and look at updating the automated process to bypass these manual components and have a new ‘trigger’ for the automated process to disable access.

Recommendation 7.2
Based on Recommendation 7.1, TEBS should update AP 6-7 and/or additional IT security policies and procedures with the defined time period for terminated user’s access to be disabled.

Recommendation 7.3

Once all policies, procedures and processes are updated based on Recommendation 7.2, TEBS should communicate and/or conduct an internal training to ensure all parties are aware of changes to existing and new policies, procedures, and processes.

Recommendation 7.4
FRS should implement processes to ensure that termination notifications are sent out the same day as an employee's termination or within 24 hours of their notice. If notifications cannot be sent out within the 24-hour period following an employee's termination, the department needs to determine a reasonable time period for notifications to be sent and communicate that throughout the department.

Recommendation 7.5
HHS and MCPD should implement processes to maintain all termination requests including, but not limited to the notifications from HR, email requests, and help desk tickets created.

Recommendation 7.6
HHS and MCPD should implement processes to ensure that all terminated employee access is removed within 24 hours of a user's termination notice, per AP 6-7, Section 13.3.1. All evidence of the removal of access should be maintained to ensure that access was removed in a timely manner.

Recommendation 7.7
HHS and MCPD should implement user access reviews, at a minimum on an annual basis, to ensure that all terminated users are removed from application user listings in and to ensure that all existing employees still need the access they are provisioned.

Comments and MCIA Evaluation

We provided all audited departments with a draft of this report for review and comment. Finance responded with comments on January 19, 2022;TEBS responded with comments on January 28, 2022. The TEBS and Finance responses have been incorporated in the report at Appendix B.

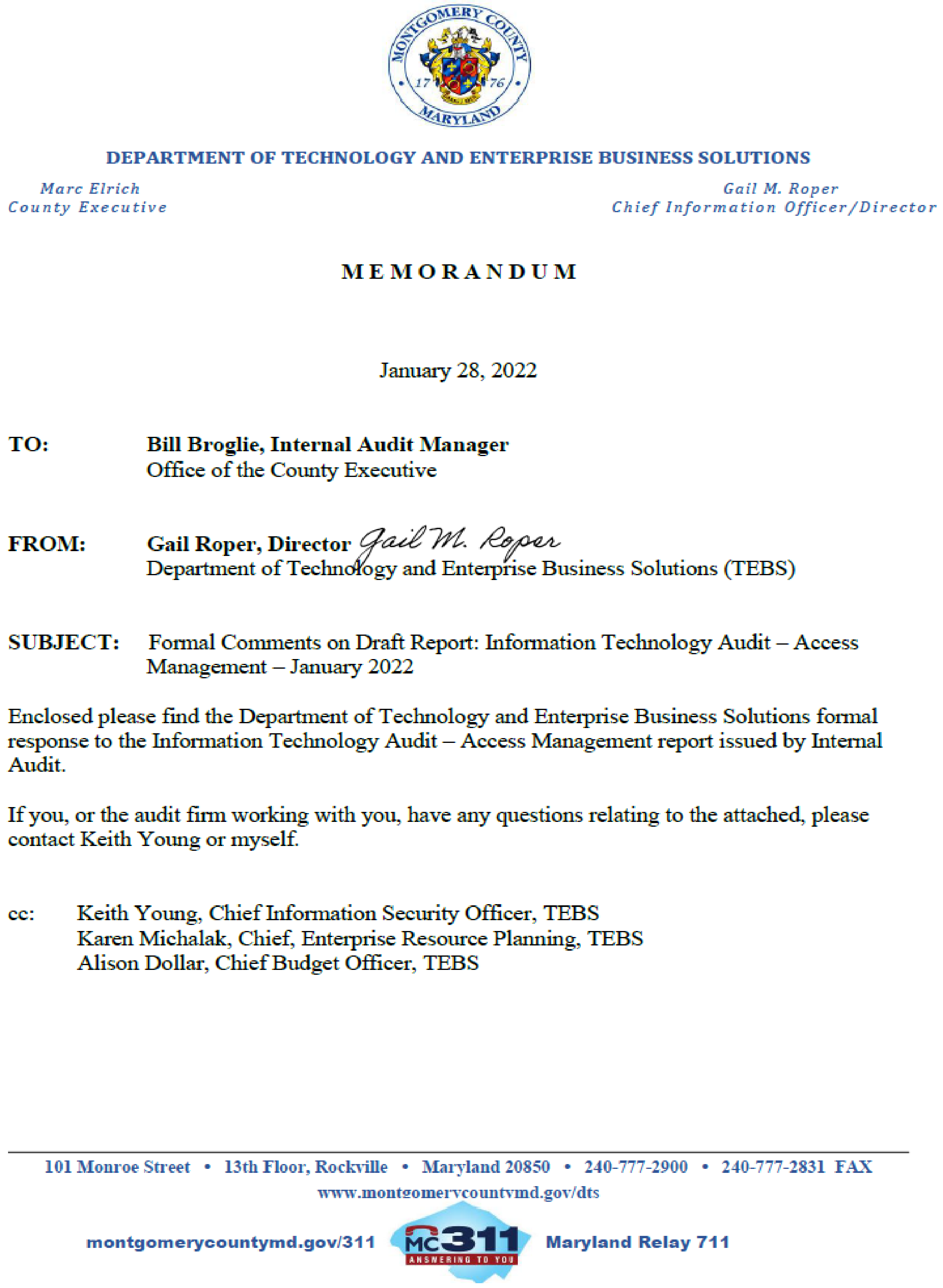
Finance acknowledged that, while it does have processes in place to follow up on requested access changes, the request identified during the course of the audit was apparently overlooked. Finance states that it has implemented a change to its procedures to address the finding, and that it is exploring additional process enhancements.

TEBS coordinated its response with the Office of Human Resources (OHR) on relevant issues. We appreciate this type of coordination across departments where findings and recommendations impact more than one department. TEBS discussed the steps it has already taken and is continuing to take as part of its continuing efforts to restrict access to sensitive data across the enterprise. TEBS raised a concern with Finding 3.1 ("Authentication Parameters" – Lockout Policy compliance), and we have revised the finding to address the valid concern raised. TEBS also raised concerns with Recommendation 5.1 ("Background Check Policy"). While we appreciate the steps TEBS has taken to establish and implement a separate background check and suitability policy and process for all TEBS new hires, in coordination with OHR, we believe TEBS can and should take additional steps countywide to encourage or require departments to implement appropriate background check policies and processes for appropriate staffs/new hires. Therefore, we have not made any changes to the report with respect to this recommendation. For other recommendations, TEBS stated that they will work to fully implement the report recommendations. No additional comments were received.

Appendix A – Access Management

Domain	Control #	Control Description
Governance	ITAC.1	Access management policies and procedures are documented, disseminated, reviewed, and updated on an annual basis. These documented procedures are utilized to implement access controls.
	ITAC.2	Authentication policies and procedures are documented, disseminated, reviewed, and updated on an annual basis. These documented procedures are utilized to implement authentication controls.
Account Management	ITAC.3	Access management policies and procedures detail the types of accounts allowed including the following areas of account management: 1. Account managers 2. Group and role membership 3. Account creation, modification, and termination 4. Separation of duties
	ITAC.4	All logical access is authorized and approved prior to access being granted in accordance with defined policies and procedures.
	ITAC.5	Access is granted following the principle of least privilege allowing only authorized access for users that is necessary to accomplish that user's job responsibilities based on their job title.
Account Identification and Authentication	ITAC.6	TEBS has documented and implemented authentication controls that restrict or limit access through the following means: 1. Enforce a limit of three (3) consecutive invalid log on attempts by a user during a fifteen (15) minute time period. When exceeded the account will automatically be locked for thirty (30) minutes or until released by an administrator. 2. Ensure that the screen locking feature is enabled on all county computers and requires a password to access device. 3. Enforces automatic termination of a user's session after defined period of inactivity.
	ITAC.7	All user accounts are created for a specific user with a unique user id and password.
Personnel Screening	ITAC.8	Background checks are required to be completed, in accordance with policy, prior to authorizing access to County Information Systems.
Terminated users	ITAC.9	All terminated employees must have their AD account disabled within 24 hours of their termination.
	ITAC.10	Access to systems that are not single sign on and/or authenticated through AD are disabled within 24 hours of termination. Application access to systems which require AD authentication are removed timely.
Transferred Users	ITAC.11	All transferred employees should have their AD access transferred to their new OU within five (5) days of their formal transfer action. Critical application access should be reviewed and adjusted as needed.

Appendix B – Department Comments



DEPARTMENT OF TECHNOLOGY AND ENTERPRISE BUSINESS SOLUTIONS

Marc Elrich
County Executive

Gail M. Roper
Chief Information Officer/Director

MEMORANDUM

January 28, 2022

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 Audit – Access Management – January 2022

Enclosed please find the Department of Technology and Enterprise Business Solutions formal response to the Information Technology Audit – Access Management report issued by Internal Audit.

If you, or the audit firm working with you, have any questions relating to the attached, please contact Keith Young or myself.

cc: Keith Young, Chief Information Security Officer, TEBS
Karen Michalak, Chief, Enterprise Resource Planning, TEBS
Alison Dollar, Chief Budget Officer, TEBS

101 Monroe Street • 13th Floor, Rockville • Maryland 20850 • 240-777-2900 • 240-777-2831 FAX
www.montgomerycountymd.gov/dts

montgomerycountymd.gov/311 MC311 ANSWERING TO YOU Maryland Relay 711

TEBS welcomes the opportunity to use the findings of this audit to increase the security of County information and to improve access management practices across County government. TEBS and all County Departments take seriously our responsibility to protect the data and systems we administer from inappropriate access. We are always working to improve the security of data, information systems, processes, and physical infrastructure. We accept and plan to implement the following recommendations:

1. Require annual review of access management policies and procedures.
2. Implement processes to ensure new access request forms are easily accessible, provide sufficient detail regarding access requested, include appropriate authorization and approval of access, and ensure roles requested follow the "least privilege needed" principle.
3. Ensure authentication guidelines implemented meet the Information Security System and Data Owners Handbook requirements.
6. Implement processes to ensure that Organization Unit (OU) transfers are requested by Departments and processed in a timely manner.
7. Implement processes to ensure that access requests associated with termination notices are processed within 24 hours of receipt of the notice.

Steps Taken or Planned to Increase Access Management Controls

TEBS has already completed significant restriction of access permissions in Office 365 using the recently acquired tool Varonis. This initiative began in 2020 and is ongoing as a continual process to restrict access to sensitive data across the Enterprise. In addition, TEBS has decreased the number of administrative accounts with access to Enterprise data and performed access reviews on the remaining administrators of critical systems. Logs of administrative actions are audited by the TEBS Office of Enterprise Information Security (OEIS) and periodic reviews of administrative privileges will continue to be conducted.

TEBS concurs with the need for an annual policy review process as well as the retention of requests to manually linked accounts and is in the process of implementing those recommendations.

As a result of the audit process, TEBS has already worked to implement an automated process that will remind Department IT staff that they must submit a ticket to transfer the OUs of employees recently transferred into their Department. TEBS will regularly monitor reports on the outstanding OU transfers.

TEBS and the Office of Human Resources (OHR) concur with finding and recommendation #7. Both Departments are working to implement short-term and long-term changes to ensure termination notices are processed within 24 hours of receipt. In the short-term, OHR and TEBS will be working to develop a report to identify the sources of the problem and educate Departments that are not meeting the security standard of 24 hours. In the long-term, TEBS and

OHR will continuously monitor compliance, notify and educate Departments about policies, track Departments that violate policy, and notify Department Directors of violations to enforce compliance.

Concerns Regarding Finding 3.1

TEBS cannot concur with finding 3.1 which states:

"In reviewing AP 6-7, with the county-wide authentication settings for AD, SC&H identified the following areas of noncompliance with the authentication parameters provided:

1. Lockout policy
2. Lockout duration"

As provided to the auditors during their assessment, the lockout duration setting for the Enterprise Active Directory (AD) is 0 minutes, not 15 minutes as stated in AP 6-7. However, the zero-minute setting is more restrictive than the policy defined duration. With this setting, a user needs an administrator to unlock their account if locked out rather than a 15-minute waiting period to be able to attempt to login again. As zero is more restrictive, and more restrictive settings are allowed by the policy, TEBS cannot concur with this finding.

The auditor's recommendation that TEBS-AD team should update all critical information systems' authentication settings to follow the documented County information security policies and procedures will not be implemented as it relates to the lockout duration as it would decrease security controls. The recommendation regarding the lockout policy will be implemented as suggested.

Concerns Regarding Recommendation 5.1

TEBS does not concur with recommendation 5.1 which reads as follows:

> "TEBS should update AP 6-7 to clearly define the screening criteria that will be utilized as part of Section 13 (e.g., credit, criminal, complete background checks, or some combination based on risk designation) to provide sufficient guidance for TEBS and all County departments that utilize AP 6-7 as their primary information technology security policy"

According to AP 6-7: "Departments must: Assign a risk designation to all County positions; Establish screening criteria for individuals filling those positions; and Review and update position risk designations every two years or as frequently as needed." "Departments must: Screen individuals prior to authorizing access to the Information System. Rescreen individuals in accordance with specific departmental requirements."

AP 6-7 is based on National Institute of Standards and Technology (NIST) standards, and intentionally left the determination of applicable screening criteria to County departments. County departments are in the best position to know what information, data, and systems their employees, interns, volunteers, and contractors have access to, the roles these individuals fulfill, what risks the department must mitigate, and therefore what background checks must be performed at the department level. In addition, multiple types of legally mandated screening and background checks may apply to the department level access of certain data types and information systems.

Using AP 6-7 as the authorizing policy, TEBS has established and implemented a separate background check and suitability policy and process for all TEBS new hires in a joint effort with OHR using jointly determined risk designations for those positions which focuses on mitigating risk to County information systems. TEBS is willing to provide the TEBS background check policy as a baseline for other departments.

OHR may choose to draft a new Countywide policy, independent of AP 6-7, to help accomplish the reduction of risk intended by this recommendation. An additional level of detail regarding background check policies would be based on a decision made by the Chief Administrative Officer (CAO) and would likely not be administered by TEBS. It is unlikely that TEBS alone can define, implement, or enforce background checks to the level suggested in this recommendation across all of County Government.

DEPARTMENT OF FINANCE

Marc Elrich
County Executive

Michael J. Coveyou
Director

MEMORANDUM

January 19, 2022

FROM: Mike Coveyou, Director
Department of Finance
Michael J Coveyou

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

SUBJECT: Formal Comments - ***Information Technology Audit – Access Management***

Thank you for the opportunity to provide a formal response to Recommendation 6.3 in the report: ***Information Technology Audit - Access Management.***

Finding - 6.2 Department of Finance (FIN)
Based on the testing performed, a transfer request ticket documenting roles that should have been removed for a transferred employee was created; however, all requested changes associated with that request were not completed for one of three samples selected. Additional details regarding the transferred employee's requests are included in separate communication directly with FIN.

Recommendation 6.3 (Lead: FIN)
FIN should ensure that all requested roles are added or removed per the access request tickets, including but not limited to ensuring that access change requests are completed in an accurate and timely manner.

Formal Response to Recommendation 6.3 (Lead: FIN)
As discussed, one change requested by Finance to remove an employee's access to a non-production read-only testing environment in a Business Intelligence (BI) reporting tool was overlooked being processed and was not caught by Finance. Finance does have processes in place to follow up on such requests; however, this one item, which was part of a larger request, was overlooked. Finance has implemented a change to its procedures to submit non-production requests only through email. This change will allow Finance to ensure that a

confirmation email indicating completion of the request is received back from the Department of Technology Enterprise Business Solutions (TEBS) Enterprise Resource Program Team (ERP) which processes such requests. In addition, Finance has discussed with ERP possible additional process improvements within that program. We would also note that, while the risks cited include unauthorized/conflicting/overlapping access to sensitive data and critical systems or exposure to unauthorized changes, in this case the employee had valid and authorized access to the exact same data in the BI reporting tool production environment, access to both production and testing environments is read-only, and access to both production and testing environments only allowed the employee to create his own reports.

We appreciate the opportunity to provide this formal response.