CITY OF RICHMOND
CITY AUDITOR

**DATE:** June 30, 2020

**TO:** Ms. Lenora Reid
Acting Chief Administrative Officer

**FROM:** Louis Lassiter LL
City Auditor

**SUBJECT:** Department of Information Technology (DIT)
User Access audit

The City Auditor's Office has completed the Information Technology User Access audit and the final report is attached.

We would like to thank the staff of DIT and HR for their cooperation and assistance during this audit.

Attachment

cc: The Richmond Audit Committee
The Richmond City Council
Todd Charles, Director of DIT
Mona Adkins-Easley, Interim HR Director

Intentionally left blank

City of

RICHMOND

Office of the City Auditor

Audit Report# **2020-14**

# Information Technology – User Access Audit

June 30, 2020

**Audit Report Staff**

Louis Lassiter, City Auditor<br>
Lily Hernandez, Deputy City Auditor<br>
Ryan Gartin, Lead Auditor

*June 2020*

# *Highlights*

*Audit Report to the Audit Committee, City Council, and the Administration*

### Why We Did This Audit

The Office of the City Auditor conducted this audit as part of the FY20 audit plan approved by the Audit Committee. The objective for this audit was to validate compliance with City policies over information systems and internal controls over user access for Active Directory and other critical City systems.

### What We Recommend

Director of Human Resources:

- Develop and implement a policy outlining the communication responsibilities for new hires and separated employees between HR and the Automation Coordinators.

Director of Information Technology:

- Revise the SAPR instructions to outline the required elements in the description field such as land line phones and mobile devices for all types of SAPR requests.
- Develop and implement a process to define the responsibilities for removing access to the RAPIDS Application.
- Develop and implement a standard process for managing and monitoring the timely completion of access control service requests and manual activities within DIT Teams.

Other recommendations to improve internal controls are included in the report.

## Information Technology - User Access Audit

**Background -** System Access Privilege Requests (SAPR) are processed for new accounts to delete accounts, application requests, transfers, and change domain accounts. Department Automation Coordinators (AC) initiate requests through an application called BonitaSoft. The Department of Information Technology (DIT) processes and manages the requests by creating Service Requests and Manual Activities in a ticket management system called Service Manager. Over 4,800 request were processed for the period audited.

### Commendation

*Separated Accounts* - Active Directory accounts for separated employees with SAPRs were all properly disabled/deleted by DIT.

*RAPIDS Application Access* - All RAPIDS responsibilities analyzed were in alignment with the employees' roles and responsibilities.

### Needs Improvement

#### Finding #1 – *Communications to Department Automation Coordinators*

*Account Setup -* The auditors analyzed 50 of 618 new hires to determine the timeliness of requesting network access account set up. In six instances, the new accounts were requested after the employees' start dates. The number of days ranged from one to six days after their start dates. HR did not have a formal process that defined the roles and responsibilities for notifying the ACs about setting up new employee accounts.

*Account Removal -* The auditors analyzed 50 of 886 separated employees to determine the timeliness of removing access to the network. In 14 of 50 instances, SAPRs to delete their access were not identified. Subsequent to obtaining the data, 10 of the 14 SAPRs were submitted and four remained un-submitted. An analysis of the 46 SAPRs revealed 38 were submitted after the employees' separation dates. 29 of the 38 were submitted more than three days after the employees' separation date. The days ranged from four to 263 days after their separation.

#### Finding #2 – SAPR Description Field Requirements

The auditors analyzed 46 Service Requests to determine if network access had been removed for separated employees. In 44 of 46, Manual Activities were assigned to the Telecommunications Team even though only seven applied to them. The SAPR form does not have a required element for actions related to the Telecommunications Team. The SAPR instructions do not outline phone requirements for "Delete Account" requests.

#### Finding #3 - End Dating Access to the RAPIDS Application

The auditors analyzed 45 of 251 users that were granted access to the RAPIDS Application and/or had access removed during the 13 months ended January 31, 2020. Of the 45 users, 28 were granted access and 17 had their access removed. A SAPR was not submitted for 11 of the 17. Additionally, the RAPIDS Application was not end dated for two former employees, who subsequently returned to the City. The lapse of time between leaving and returning to City employment ranged from 30 to 60 months. Another former employee who separated in July 2019, still had access to the RAPIDS Application.

#### Finding #4 – Service Requests and Manual Activities

The auditors analyzed the timelines for the completion of Service Request and Manual Activities opened during the 13 months ended January 31, 2020. The analysis revealed that 30% of Service Requests and 25% of Manual Activities were not closed within three days as established by DIT's Operating procedures. The completed Manual Activities that exceeded three business days ranged from four to 137 days. Some of the delays were due to staff turnover, inconsistent methods of managing SRs and ineffective monitoring process.

Management concurred with 7 of 7 recommendations. We appreciate the cooperation received from management and staff while conducting this audit.

# BACKGROUND, OBJECTIVES, SCOPE, METHODOLOGY, MANAGEMENT RESPONSIBILITY and INTERNAL CONTROLS

This audit was conducted in accordance with the Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States. Those Standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objectives.

## BACKGROUND

System Access Privilege Requests (SAPR) are processed for new accounts, delete accounts, application requests, transfers, and change domain accounts. Department Automation Coordinators (AC) initiate requests through an application called BonitaSoft. The Department of Information Technology (DIT) processes and manages the requests by creating Service Requests and Manual Activities in a ticket management software called Service Manager. The following table depicts the number and type of requests submitted during the audit scope:

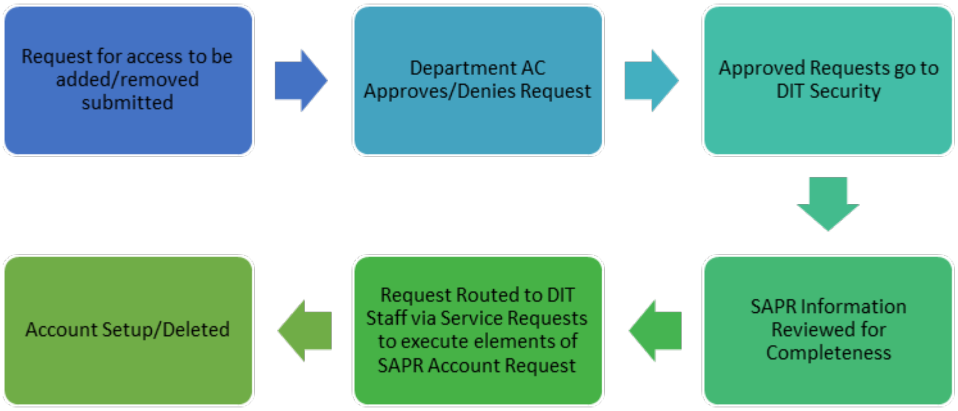
| SAPR Type | Number of SAPRs |
|---|---|
| New Account | 1,097 |
| Delete Account | 963 |
| Change Domain Account | 956 |
| Transfer | 105 |
| Application Requests | 1,703 |

Auditor Prepared

*<u>SAPR Process</u>*

Each department's AC is responsible for submitting the SAPRs for the employees within his/her department. The following flowchart illustrates the setup and/or removal of accounts:

New Account/Delete Account Requests

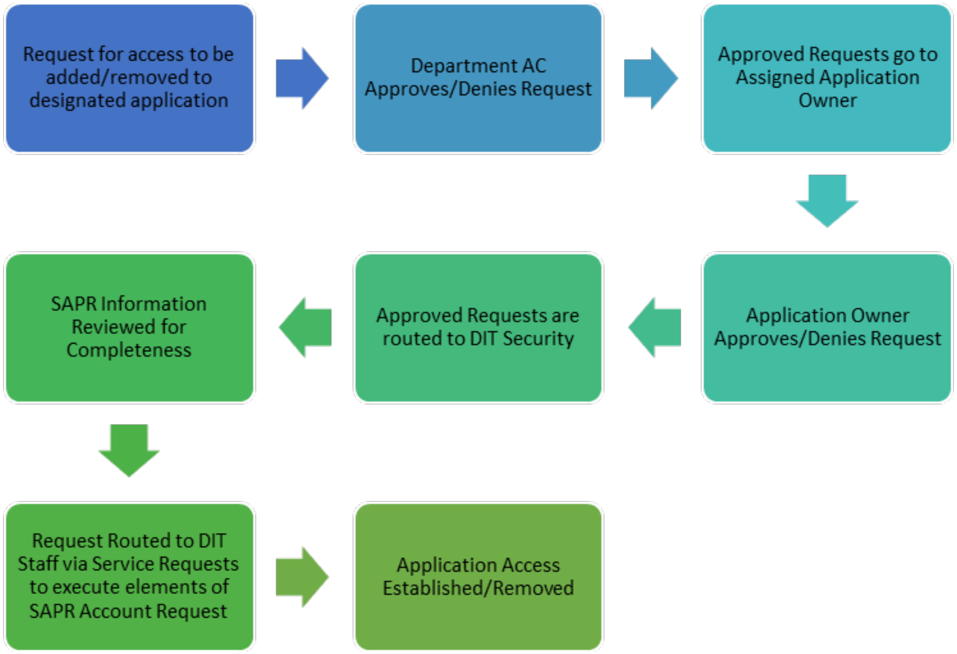

Request for access to be added/removed submitted
Department AC Approves/Denies Request
Approved Requests go to DIT Security
SAPR Information Reviewed for Completeness
Request Routed to DIT Staff via Service Requests to execute elements of SAPR Account Request
Account Setup/Deleted

Auditor Prepared Chart

*Application Access Requests and Application Owners*

City departments use a variety of software applications to conduct their work. While DIT is the system administrator for many applications, some applications are managed by the departments. For access to the applications managed by DIT, each application has an assigned owner that approves access requests. The following flowchart illustrates the process for submitting application access requests to DIT:

Application Access Requests

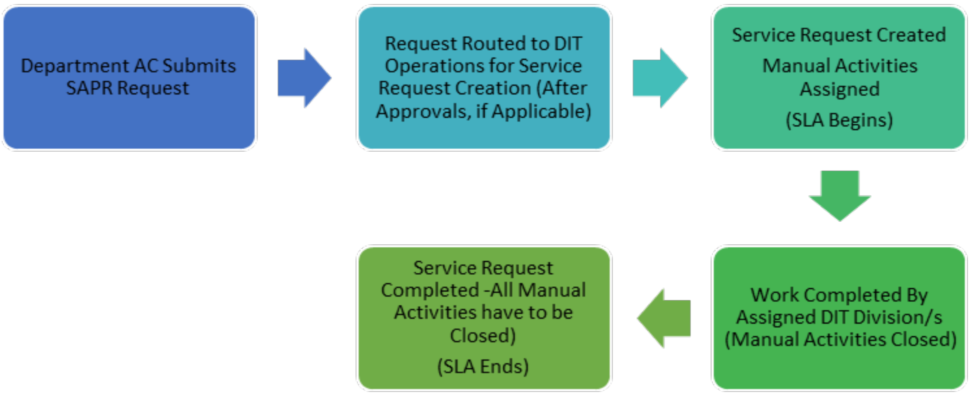

Request for access to be added/removed to designated application
Department AC Approves/Denies Request
Approved Requests go to Assigned Application Owner
Application Owner Approves/Denies Request
Approved Requests are routed to DIT Security
SAPR Information Reviewed for Completeness
Request Routed to DIT Staff via Service Requests to execute elements of SAPR Account Request
Application Access Established/Removed

Auditor Prepared Chart

*Service Requests and Manual Activities*

DIT implemented Service Manager on 7/1/2018 to manage Service Requests for access control among all other types of requests/incidents submitted to them, which allows automated and manual workflows. DIT has an established Service Level Agreement (SLA) of three business days for medium priority Service Requests.

Once DIT receives a SAPR, their Security Team creates a Service Request in Service Manager and assigns Manual Activities to their teams for executing the work. The Manual Activities are assigned and routed to each DIT area based on the provided description in the SAPR. DIT Security is notified as the teams complete the activities. The Service Requests and the SAPRs are closed once all the Manual Activities are completed. This process is illustrated in the following flowchart:


Department AC Submits SAPR Request
Request Routed to DIT Operations for Service Request Creation (After Approvals, if Applicable)
Service Request Created
Manual Activities Assigned
(SLA Begins)
Work Completed By Assigned DIT Division/s (Manual Activities Closed)
Service Request Completed -All Manual Activities have to be Closed)
(SLA Ends)

## OBJECTIVES

The objective for this audit was to validate compliance with City policies over information systems and internal controls over user access for Active Directory and other critical City systems.

## SCOPE

All granting and revoking of user access to employees, vendors, and any other external party requiring access to the City's network and the RAPIDS Application during the 13 months ended January 31, 2020.

## METHODOLOGY

The auditors performed the following procedures to complete this audit:

- Interviewed staff;
- Reviewed and evaluated relevant City of Richmond policies and procedures for compliance;
- Analyzed and reviewed SAPR requests;
- Analyzed and reviewed access control Service Requests and Manual Activities;
- Analyzed timelines for DIT Service Level Agreements; and
- Performed other tests, as deemed necessary.

## MANAGEMENT RESPONSIBILITY

City of Richmond management is responsible for ensuring resources are managed properly and used in compliance with laws and regulations; programs are achieving their objectives; and services are being provided efficiently, effectively, and economically.

## INTERNAL CONTROLS

According to the Government Auditing Standards, internal control, in the broadest sense, encompasses the agency's plan, policies, procedures, methods, and processes adopted by management to meet its mission, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It also includes systems for measuring, reporting, and monitoring program performance. An effective control structure is one that provides reasonable assurance regarding:

- Efficiency and effectiveness of operations;
- Accurate financial reporting; and
- Compliance with laws and regulations.

Based on the audit test work, the auditors concluded the internal controls over the IT User Access need improvement.

# FINDINGS and RECOMMENDATIONS

## What Works Well

- Separated Accounts - Active Directory Accounts for separated employees with SAPRs were all properly disabled/deleted by DIT.
- RAPIDS Application Access - All RAPIDS responsibilities analyzed were in alignment with the job descriptions of the employees tested.

## What Needs Improvement

### *Finding #1 –Communications to Department Automation Coordinators*

*Account Setup*

The auditors analyzed 50 of 618 new hires to determine the timeliness of requesting network access account set up. In six instances, the new accounts were requested after the employees' start dates. The number of days ranged from one to six days after the employees' start dates.

The auditors noted HR did not have a formal process that defined the roles and responsibilities for notifying the ACs about setting up new employee accounts. As a result, the notification process between HR and the ACs was inconsistent. The ACs indicated they received information from various sources within the City. Policies and procedures would guide employees to perform their duties consistently in conformance with policies.

Additionally, untimely access to the network and systems may result in loss of productivity as employees may not be able to execute their job duties. Without a formal policy and procedures, management's intent may not be carried out.

*Account Removal*

The auditors analyzed 50 of 886 employees who separated from the City to determine the timeliness for removing their network access. In 14 of 50 instances, SAPRs to delete employees' access were not identified in the data extracted by the auditors on February 24, 2020. Subsequent to that date, 10 of the 14 SAPRs were submitted by the departments' ACs and four remained un-submitted.

An analysis of the 46 SAPRs revealed:

- 8 were submitted prior to the employees' separation dates.
- 38 were submitted after the employees' separation dates.

- o 29 of the 38 were submitted more than three days after the employees' separation dates. The days ranged from four to 263 days after their separation dates.

The auditors also noted that for 32 of 50 separated employees, HR could not provide documentation to demonstrate their communication with the ACs. The documentation provided for the 18 demonstrated inconsistent processes among the departments.

Written policies and procedures to guide the communication process between HR staff and the departments' ACs to remove former employees' accounts were not in place. HR did not have a formal process to delineate the roles and responsibilities to notify the ACs about separations. Without guidance, the automation coordinators were left to interpret the timeliness and urgency of submitting SAPRs for separated employees. Separated employee accounts remained active, which resulted in retaining access to the system after they leave employment.

Recommendation:

1. *We recommend the Director of Human Resources develop and implement a policy outlining the communication responsibilities for new hires and separated employees between HR and the Automation Coordinators.*

## *Finding #2 – SAPR Description Field Requirements*

The auditors analyzed 46 Service Requests to determine if network access had been removed for separated employees. In 44 of the 46, Manual Activities were assigned to the Telecommunications Team. The analysis revealed only seven of the 44 SAPRs included telecommunications needs.

The SAPR form does not have a required element for actions related to the Telecommunications Team, such as land lines and mobile devices. Also, the SAPR instructions do not outline phone requirements for "Delete Account" requests. SAPR forms should be designed to promote efficiency and accuracy in the SAPR submittal process. As a result, Manual Activities were created for the Telecommunications Team although they did not have outlined work. This creates inefficiencies and untimely completion of the requests.

Recommendations:

2. *We recommend the Director of Information Technology revise the SAPR instructions to outline the required elements in the description field such as land line phones and mobile devices for all types of SAPR requests.*

3. *We recommend the Director of Information Technology train automation coordinators on updated SAPR instructions.*

## *Finding #3 – End Dating Access to the RAPIDS Application*

The auditors analyzed 45 of 251 users that were granted access to the RAPIDS application and/or had access removed during the 13 months ended January 31, 2020. Of the 45 users:

- 28 users were granted access to the RAPIDS Application.
- 17 users had their RAPIDS access removed.

The analysis revealed that a SAPR was not submitted for 11 of the 17 users that had their access removed.

Additionally, the auditors noted access to the RAPIDS Application was not end dated for two employees who had left City employment. These employees subsequently returned to the City. Their lapse of time between leaving and returning to City employment ranged from 30 to 60 months. Another former employee who separated in July 2019, still had access to the RAPIDS Application.

The auditors also noted the ACs did not have specific guidance on how to submit access removal for the RAPIDS Application. Without formal guidance related to the responsibilities of end dating access to the RAPIDS Application, users' access may not be removed and they could continue to access the application after separating from City employment. Written policies and procedures provide guidance to staff to perform their duties consistently in conformance with policies.

According to the DIT RAPIDS' System Administrator, they run daily reports of separated employees to remove their access. However, this process was not always effective.

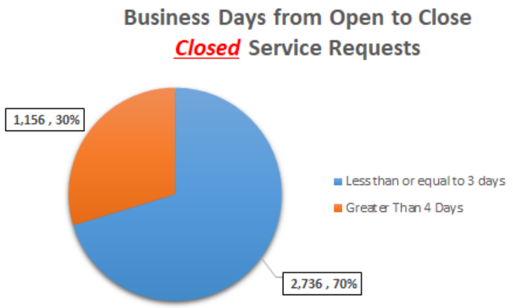
Recommendations:

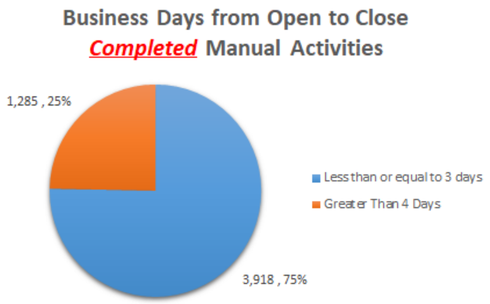
4. *We recommend the Director of Information Technology develop and implement a process to define the responsibilities for removing access to the RAPIDS Application.*
5. *We recommend the Director of Information Technology provide training to Automation Coordinators on the updated RAPIDS access removal process.*

## *Finding #4 – Service Requests and Manual Activities*

The auditors analyzed the timelines for the completion of Service Requests and Manual Activities opened during the 13 months ended January 31, 2020. The analysis revealed that 30% of Service Requests and 25% of Manual Activities were not closed within three business days as established by DIT's SLAs. According to DIT's End User Services Standard Operating Procedure and Service Request SLA Matrix, access control requests should be completed within three business days.

The completed Manual Activities that exceeded three business days ranged from four to 137 days. The results of the analysis are depicted in the following graphs:





Based on walkthroughs and inquiries with DIT staff, the following reasons were identified as delays in processing access control Service Requests:

- Staff turnover and the transfer of knowledge within DIT Teams caused delays in processing Service Requests and Manual Activities.
- Inconsistent methods of managing Service Requests by the DIT teams.
- Ineffective monitoring procedures.
- Calculations in the DIT reports did not align with the SLAs as it counts total days rather than business days.

As a result, Service Requests and Manual Activities were not completed in a timely manner, which may lead to:

- New accounts not being established timely.
- Separated employee accounts not being disabled/deactivated timely.

Recommendations:

6. *We recommend the Director of Information Technology revise the access control Service Level Agreement report to calculate the duration of completing service requests based on business days.*

7. *We recommend the Director of Information Technology develop and implement a standard process for managing and monitoring the timely completion of access control service requests and manual activities within DIT Teams.*

## APPENDIX A: MANAGEMENT RESPONSE FORM

## 2020-14 Information Technology - User Access Audit

| | | | |
|---|---|---|---|
| **#** | **RECOMMENDATION** | **CONCUR Y/N** | **ACTION STEPS** |
| **1** | We recommend the Director of Human Resources develop and implement a policy outlining the communication responsibilities for new hires and separated employees between HR and the Automation Coordinators. | **Y** | HR will draft a policy outlining the communication responsibilities for new hires and separated employees between HR and the Automation coordinators. |
| #REF! | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| #REF! | Program and Operations Supervisors | | 7/15/2020 |
| #REF! | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| #REF! | | | |
| **#** | **RECOMMENDATION** | **CONCUR Y/N** | **ACTION STEPS** |
| **2** | We recommend the Director of Information Technology revise the SAPR instructions to outline the required elements in the description field such as land line phones and mobile devices for all types of SAPR requests. | **Y** | The Department will update the input forms in the current tool (BonitaSoft). |
| #REF! | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| #REF! | IT Manager for Application Solutions | | 9/30/2020 |
| #REF! | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| #REF! | | | |
| **#** | **RECOMMENDATION** | **CONCUR Y/N** | **ACTION STEPS** |
| **3** | We recommend the Director of Information Technology train automation coordinators on updated SAPR instructions. | **Y** | The Department will offer stand-alone sessions on this topic and add to the agenda of regular Automation Coordinator meetings. |
| #REF! | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| #REF! | IT Strategy Resource / Program Manager | | 9/30/2020 |
| #REF! | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| #REF! | | | |
| **#** | **RECOMMENDATION** | **CONCUR Y/N** | **ACTION STEPS** |
| **4** | We recommend the Director of Information Technology develop and implement a process to define the responsibilities for removing access to the RAPIDS Application. | **Y** | The Department will create a process providing for the end-dating / removal of a user's access to RAPIDS when DIT determines that a separated employee still has access to the application. The process will also cover how that determination is made. |
| #REF! | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| #REF! | IT Manager for Application Solutions | | 9/30/2020 |
| #REF! | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| #REF! | | | |
| **#** | **RECOMMENDATION** | **CONCUR Y/N** | **ACTION STEPS** |
| **5** | We recommend the Director of Information Technology provide training to Automation Coordinators on the updated RAPIDS access removal process. | **Y** | The DIT and the RAPIDS owner will create and offer this training after item 4 is completed. |
| #REF! | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| #REF! | DIT Director | | 9/30/2020 |
| #REF! | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| #REF! | | | |

## APPENDIX A: MANAGEMENT RESPONSE FORM

## 2020-14 Information Technology - User Access Audit

| | | | |
|---|---|---|---|
| **#** | **RECOMMENDATION** | **CONCUR Y/N** | **ACTION STEPS** |
| **6** | We recommend the Director of Information Technology revise the access control Service Level Agreement report to calculate the duration of completing service requests based on business days. | **Y** | If the DIT ticketing system is capable of calculating on business days rather than calendar days, DIT will make the change. |
| #REF! | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| #REF! | IT Manager for End User Service | | 9/30/2020 |
| #REF! | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| #REF! | | | |
| **#** | **RECOMMENDATION** | **CONCUR Y/N** | **ACTION STEPS** |
| **7** | We recommend the Director of Information Technology develop and implement a standard process for managing and monitoring the timely completion of access control service requests and manual activities within DIT Teams. | **Y** | There is already a report every Tuesday listing all open service requests. DIT will identify a means to extract access management requests to focus on them. |
| #REF! | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| #REF! | IT Manager for Application Solutions | | 9/30/2020 |
| #REF! | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| #REF! | | | |