Active Directory

Internal Audit Report – # 21121

Bobby Mukundan, SVP, Enterprise Technology Services (ETS)
Chandra McMahon, Chief Information Security Officer, Enterprise Information Security (EIS) April 5, 2022

I. AUDIT BACKGROUND

CVS Health uses Windows Active Directory (AD) technology directory service to centrally store and manage security principals, such as users, groups, and computers, and it offers centralized and secure access to network resources. AD's primary function is to authenticate and approve the action that a user is trying to perform, either on the network or locally.

AD Domain Controllers control the various users and computers within the controller's scope. Establishing the proper security configuration settings during AD implementation and maintaining those configurations is critical to ensure user credentials, company systems and sensitive data remain protected. As of November 2021, the CVS Enterprise contains 25 domains and 342 Domain Controllers all of which are managed by the Enterprise Technology Services Team. There are approximately 582K users managed within these domains.

A security compromise of AD can undermine the integrity of CVS Health's identity management infrastructure, leading to data leakage and/or system corruption/destruction.

II. SCOPE & OBJECTIVES

The objective of this audit is to provide assurance of the Active Directory implementation and management security design effectiveness. In addition, provide assessment of the operating effectiveness of the security controls.

The scope included the following objectives, for the period of November 2021 through January 2022:

A. Active Directory Management
B. Secure Active Directory Boundaries
C. Secure Domain Controllers
D. Active Directory Administrative Practices
E. Logging and Monitoring

III. CONCLUSION & FINDINGS SUMMARY

☐ **Effective**	☒ **Mostly Effective**	☐ **Improvement Needed**	☐ **Ineffective**

Based on the procedures performed for this audit, except for the issues noted below, controls in place over the Active Directory implementation and management security design effectiveness provide reasonable assurance that the business risks reviewed are adequately mitigated.

Description	Business Area	Rating	Ref. to Objective
Finding			
1. AD Privileged Access Review (PAR)	ETS	Medium	A
Observation			
1. Standard Operating Procedures (SOPs)	ETS	Observation	A
2. Known Active Directory Issues	ETS	Observation	A

IV. FINDINGS & MANAGEMENT ACTION PLANS

1. AD Privileged Access Review

Per CVS Health Periodic Access Review (PAR) Control Standard (ACS-988), CVS Health shall periodically review user access related to applications, operating system platforms, and databases designated as critical for CVS Health to meet regulatory, compliance, or contractual obligations. Reviews shall be facilitated by the PAR owner for all users with access to sensitive data classified applications and systems. AD High Privileged user accounts managed by the AD Engineering Team are expected to follow a semi-annual review cycle based on the classification outlined in ACS-988.

IA evaluated the latest PAR cycle completed (Q4 2021), to ensure the AD Engineering identified 18 privileged user groups were included. Based on review, 5 of 18 AD privileged groups were not included in the semi-annual review as expected based on the control standard ACS-988. IA performed further analysis on the 5 privileged groups and found the following:

- 2 privileged group owners were terminated and would be unable to fullfill ownership responsibilities, including user account review.
- 1 group owner and 8 user accounts belong to non EIS or ETS AD support which appear inappropriate based on job responsibilities.

Without a complete AD privileged user group list provided by AD Engineering Team for inclusion in the PAR process, access to AD may not be adequately monitored and could result in unauthorized access.

IA recommends the AD Engineering Team ensure all AD privileged user accounts are provided for inclusion in the PAR process.

Rating: Medium

Management Action Plan:

As noted in the submission of "Known Issues" at the start of this audit by ETS AD Team, the evaluation and remediation of domain privileged accounts is currently in progress with EIS. The finding uncovered High Privilege groups that were not certified via the PAR Process. To address this finding the AD team will:

- Take responsibility from the Server Engineering team to submit groups to EIS for PAR processing.
- Send a comprehensive High Privilege group listing to the PAR team for inclusion in the next PAR planned for 2022 based on existing process/timelines.
- Build out a Control Procedure to be attached to CVS Health PAR for Applications, Operating Systems, and Databases Control Standard (ACS-988).

Remediation Owner: Mark Ostrowski, Senior. Manager ETS
Jim Rose, Lead Director, ETS

Due Date: June 30, 2022
Remediation Due Date: July 16, 2022

V. OBSERVATIONS

Internal Audit identified the following opportunities to enhance management's processes.

1. Standard Operating Procedures

Critical AD SOPs provide team members with direction to follow while performing day to day responsibilities, such as commissioning and decommissioning domains/domain controllers (DCs), managing Group Policy Objects (GPOs) and handling support calls for identified events and/or outages.

Based on review, the following was noted:

- DC Replacement procedures provided by the AD Engineering team defined details and steps around replacing a DC by promoting a new DC and removing the old one, however, the document lacks formality (i.e. ownership, revision history, review cadence)
- MSB SOP referenced by the AD Engineering Team to implement Windows Server/Workstation outlines roles and responsibilities; however, lacks instruction related to performing the implementation.
- Guidance and procedures for managing GPO modification and handling support calls for identified events and/or outages were not documented and therefore could not be reviewed.

Without proper guidance and support in place for the AD Engineering team members to leverage, there is a risk of adverse service delivery while working on problem resolution and daily business functions.

IA recommends the AD team enhance and formalize existing documentation to manage critical processes Enhancements to consider includes ownership, revision history, evidence of periodic review, guidance to handle support calls (i.e. outages), and DC/GPO modifications.

2. Known Active Directory Issues

The ETS AD Team shared 3 self-identified known issues during the audit planning stage; however, the issues did not have a start date when first identified, responsible party, a risk statement, mitigating control, and had open-ended target completion date. Issues highlighted:

- Active Directory Health, Risk, and Security Assessment: Project started in late 2019. AD team worked with Microsoft to review assessment data and help guide on recommendations and remediation
- Enterprise Configurations: Implement recommended security and configuration settings which may have Business and application impact.
- Privileged Domain Access: Evaluation and remediation of domain privileged accounts to reduce Enterprise risk and utilize least privileged access.

Without a documented risk statement, mitigating controls, responsible party, or a closure date, there is no assurance the items will be remediated to address the known issues.

IA recommends the AD team fully document the known issues to include at minimum, date first identified, risk statement, mitigating or compensating controls, responsible party, and target completion date for tracking.

VI. STANDARD TERMINOLOGY

Overall Control Environment Opinion:

Effective	Overall, controls are appropriately designed and functioning as intended. Control weaknesses, if noted, do not threaten the effectiveness of the process reviewed.
Mostly Effective	Except for the issues noted, controls in place provide reasonable assurance that business risks are adequately mitigated.
Improvement Needed	One or more significant control weaknesses exist that require prompt action to prevent the process from becoming ineffective.
Ineffective	Control weaknesses are pervasive or one weakness is so severe that it impacts the entire operation under review. Immediate management attention is needed to remediate the finding identified.

Rating:

Low	The identified risk does not warrant immediate attention; however, there should be an agreed-upon action plan for ultimate resolution.
Medium	The identified risk requires the near-term attention of the responsible manager. There should be an agreed-upon action plan for its resolution.

High	The identified risk requires the immediate attention of department and senior management to prevent the process from becoming ineffective, and an agreed-upon action plan for resolution is needed.
Deficiency	If SOX related, rating categories will be assessed as Deficiency, Significant Deficiency, or Material Weakness.

Other:

Remediation Due Date	Reflects the time required for Management to complete the agreed upon action plan, as well as time for IA to complete the associated validation procedures to ensure the action plan has been implemented effectively.

VII. DISTRIBUTION LIST

Executive Leadership Team
Karen Lynch
David Falkowski
Shawn Guertin
Tom Moriarty
Jon Roberts

Office of the CIO
Roshan Navagamuwa

Finance
Jim Clark
John Maroney
Carol DeNale

Compliance
Tom Pawlik

Legal
Anna Shimanek

Enterprise Information Security
Brad Abreu
Gehan Dabare
Gary Francis
Michael Shanahan

Enterprise Technology Services
Nicole Frazier
Anne Marie French
David Kaemmerer
Bianca Moon
Terry Newman
Mark Ostrowski
Jim Rose

Internal Audit
David Chavez
Lynn Atkin
Tyrell Jarrett
Sarah Kubiak
Seun Mafi
Terri Ann Quiambao
Joseph Rocha
Ronald Roy
Emely Santos
Saurabh Saxena

External Audit
Allison Capprini
Tom Derkacs
Mike Fischer
Ryan Murphy