CVS Health®

21121 – Active Directory Audit

Status Update

02/04/2022

AGENDA

Project Status

Walkthroughs & Meetings

Data Requests

Initial Observations

Appendix

- Engagement Details
- Audit Timeline

Audit Progress – Current Status

The audit is currently in the Testing and Fieldwork Phase.
Audit is expected to be completed on time. | There is one discovery identified at this time.

Milestones	Timing*	Status	Comments
Planning Phase			
Conduct Kick-Off Meeting	11/30/21	✓	
Control Analysis Phase			
Conduct Walkthroughs	12/08/21	✓	
Validate Risk Control Analysis	12/31/21	✓	**Actual control analysis end date 1/20/22. As a result of the business prioritizing and addressing security issues and ETS organizational changes.**
Fieldwork Phase			
Testing Execution	01/31/22	**In Progress**	**5 out of 13 controls testing on-going**
Reporting Phase			
Validation of Findings (if applicable)	02/04/22	**In Progress**	
Management Action Plan (MAP)	02/11/22	**On Track**	
Distribute Audit Report	02/28/22	**On Track**	

*Completion date

G	On Track	Y	At Risk / Recoverable	R	High Risk / Missed	✓	Complete

Walkthroughs & Meetings

Meeting Schedules					
#	Meeting Topic	Scheduled Date	Status	Attendees	Notes
1	Scope and Objective Alignment Meeting	11/18/2021	Completed	Mark Ostrowski, Julie Gonzalez, David Kaemmerer, Bianca Moon, Nicole Frazier	IA reviewed the scope and objectives with the AD infrastructure team that were finalized based on the information gathering sessions
2	AD Management	11/29/2021	Completed	Jim Rose, Anne Marie French, Julie Gonzalez, Bianca Moon, Nicole Frazier	Topics covered during the meeting with AD infrastructure team: • Policies and Procedures which cover AD management processes • Clearly defined roles and responsibilities for AD administration • Management reporting of problems, changes, incidents etc.
3	Secure AD Boundaries	12/1/2021	Completed	Jim Rose, Anne Marie French, Julie Gonzalez, Bianca Moon, Nicole Frazier	Topics covered during the meeting with AD infrastructure team: • Review AD design and structure (i.e. Domains, Trees, Forests, Organizational Units (OU)) • Review Segregation of Duties exists for critical AD functions like Administration, Monitoring, Making Changes etc. • Review Domain Trusts relationship
4	Secure Domain Controller	12/3/2021	Completed	Jim Rose, Anne Marie French, Julie Gonzalez, Bianca Moon, Nicole Frazier	Topics covered during the meeting with AD Infrastructure colleagues: • Review documented AD Domain Controller installation procedures and processes • Availability of Domain Controllers • Regular updates of Service Packs • Change management procedures associated with AD configurations settings which include Group Policy Objects (GPO) and Organizational Unit management
5	Administrative Practices	12/6/2021	Completed	Jim Rose, Anne Marie French, Julie Gonzalez, Bianca Moon, Nicole Frazier	Topics covered during the meeting with AD infrastructure team: • Administrator Account Limitations are based on job responsibilities. • Separate accounts for administrative and non-administrative operations
6	Logging and Monitoring	12/8/2021	Completed	Mark Ostrowski, Jim Rose, Anne Marie French, Bianca Moon, Nicole Frazier, Mike Shanahan, Ryan Evans, Ryan Greene, Todd Savoy	Topics covered during the meeting with AD infrastructure team: • Evaluate AD Domain Controller Policy and Procedure requirements related to event, activity, logging and review • Review AD Domain Controller Monitoring activities for completeness

Walkthroughs & Meetings

Meeting Schedules					
#	Meeting Topic	Scheduled Date	Status	Attendees	Notes
7	Data Request Discussion	12/20/2021	Completed	Mark Ostrowski, Jim Rose, Anne Marie French, Bianca Moon, Nicole Frazier	Meeting was scheduled to go over the data request and expectations around due dates for these request were ascertained.
8	Levels of Admin Rights	1/4/2022	Completed	Mark Ostrowski, Jim Rose, Bianca Moon, Nicole Frazier, David Kaemmerer	Meeting was scheduled to understand what other levels of admin rights are configured and who/which team has access to these rights. Conversation followed after UID #13195.
9	AD Change Management Procedure	1/10/2022	Completed	Mark Ostrowski, Bianca Moon, Julie Gonzalez, David Kaemmerer	This meeting was scheduled to better understand the latest modifications (Changes to Domain, Domain controllers, GPOs, OUs) that have occurred in the Active Directory and the change management process executed by the AD infrastructure team.
10	AD Change Management Discussion- Follow up	1/14/2022	Completed	Mark Ostrowski, Bianca Moon, Julie Gonzalez, David Kaemmerer	This meeting was scheduled to discuss if there was an easier way to determine samples to test the change management procedures
11	Follow up Questions	1/20/2022	Completed	Mark Ostrowski, Bianca Moon, Julie Gonzalez, David Kaemmerer	The meeting was scheduled to go over several follow up questions which would help us document the test procedures of several control areas.
12	Domain Trust Relationship – Follow up	1/21/2022	Completed	Jim Rose, Mark Ostrowski, Nicole Frazxier, Bianca Moon, Julie Gonzalez,	This meeting was scheduled to go over the Domain Trust relationships and better understand how two way and one way domain trust relationships are established leveraging the AD Domain Trust diagram.
13	Administrative Accounts :UID 14834	1/27/2022	Completed	Jim Rose	Jim performed a screenshare session to provide us with the required screenshots in order to complete testing and document Control D.1
14	AD Change Management Data Request	1/28/2022	Completed	Jim Rose	This meeting was scheduled to go over in detail the change management procedures carried out by the AD Infrastructure team.
15	DC Advanced Audit Settings Discussion	2/3/2022	Completed	Ann Marie French, James Rose, Nicole Frazier, David Kaemmerer	Meeting is scheduled to discuss the Domain Controller Advanced Audit settings for the 10 configuration settings showing (no auditing) and as a result do not provide the AD team with relevant alerts.
16	AD High Privileged Users	2/3/2022	Completed	Brad Abreu, James Rose, Nicole Frazier, David Kaemmerer, Bianca Moon	Meeting was scheduled to discuss the PARs performed for AD High Privelege User Groups.

Data Requests

As of 5 PM ET on 2/3

Data Requests							
#	UID	Title	Started On	Due (Date)	Status	Preparer(s)	Notes
01	13200	Walkthroughs and Related Documentation (Logging and Monitoring)	12/15/2021	12/21/2021	Closed	Jim Rose	
02	13730	AD Management - Monthly AD Stat Sheet	12/21/2021	12/22/2021	Closed	Jim Rose	
03	14251	Secure AD Boundaries - Architectural Diagram	12/21/2021	12/22/2021	Closed	Jim Rose	
04	13195	Admin Access	12/15/2021	12/23/2021	Closed	Jim Rose	
05	13206	Security of Domain Controllers- Comm / Decomm of DC	12/16/2021	12/23/2021	Closed	Jim Rose	
06	13216	AD Administrative Practices - Admin Functions	12/17/2021	12/23/2021	Closed	Jim Rose	
07	13199	Security of Domain Controllers: DC Redundancy	12/16/2021	12/29/2021	Closed	Jim Rose	
08	13732	System Downtime/Outage	12/21/2021	12/29/2021	Closed	Jim Rose	
09	14252	Secure AD Boundaries - Domain Trust Relationship	12/21/2021	12/29/2021	Closed	Jim Rose	
10	14266	Secure AD Boundaries - Domain Trust Relationship (Follow-Up)	12/27/2021	1/3/2022	Closed	Jim Rose	

Data Requests

As of 5 PM ET on 2/3

Data Requests							
#	UID	Title	Started On	Due (Date)	Status	Preparer(s)	Notes
11	13731	AD Management - Reporting Metrics	12/20/2021	1/7/2022	Closed	Jim Rose	
12	14374	A1.2 - Access to Active Directory	1/4/2022	1/7/2022	Closed	Jim Rose	
13	14375	B1.2 Domain Trust Relationship	1/4/2022	1/7/2022	Closed	Jim Rose	
14	14381	C1.3 - Change Management Procedures	1/6/2022	1/11/2022	Closed	Jim Rose	
15	14365	C1.2 - Patch Updates	1/7/2022	1/12/2022	Closed	Jim Rose	
16	14721	A1.1 Standard Operating Procedures	1/10/2022	1/12/20220	Closed	Jim Rose	
17	14776	C1.2 - Patch Updates - Samples	1/10/2022	1/13/2022	Closed	Jim Rose	
18	14777	C1.1 - Domain Controller Availability (Follow Up)	1/10/2022	1/13/2022	Closed	Mark Ostrowski	
19	14782	B1.2 Domain Trust Relationship (Follow Up)	1/10/2022	1/13/2022	Closed	Mark Ostrowski	

Data Requests

As of 5 PM ET on 2/3

Data Requests							
#	UID	Title	Started On	Due (Date)	Status	Preparer(s)	Notes
20	14784	C1.3 – Change Management – Splunk Log Request	1/21/2022	1/24/2022	Closed	Mark Ostrowski	
21	14800	C1.3 – Change Management Procedures	1/18/2022	1/20/2022	Closed	Ann French	
22	14834	D1.1 – Administrative Accounts	1/21/2022	1/25/2022	Closed	Mark Ostrowski	
23	14854	B1.3 – Segregation of Duties	1/25/2022	1/27/2022	Closed	Jim Rose	
24	14856	Active Directory Trusts	1/24/2022	1/26/2022	Closed	Jim Rose	
25	14857	E2.1 Administrative Activity Logging and Monitoring	1/24/2022	2/4/2022	**Open**	Jim Rose	
26	15122	C1.3 - Trust Removal System Log	1/28/2022	1/28/2022	**Open**	Jim Rose	
27	15123	C1.3 - SOC Alerts for Admin Activity	1/28/2022	1/31/2022	Closed	Jim Rose	
28	15125	C1.3 - Server Logs for Sample DCs	1/28/2022	1/31/2022	Closed	Jim Rose	
29	15133	E2.2 SCOM Event Logs	1/28/2022	1/31/2022	Closed	Jim Rose	
30	15135	E2.2 Event Monitoring	1/31/2022	2/1/2022	Closed	Jim Rose	
31	15416	E2.2 SCOM Alerts Follow Up	2/3/2022	2/3/2022	**Open**	Jim Rose	

Potential Discovery Identified

The following discoveries were identified and will be discussed with applicable business owners to ensure alignment. These are considered draft and subject to change until the final report is issued.

Initial Discovery			
#	Discovery	IA Comment /Recommendation	Business Comment
1	IA requested standard operating procedures for critical Active Directory functions such as commissioning and decommissioning domains/domain controllers, managing Group Policy Objects (GPOs) and change management. IA noted the AD Team utilizes the standard Change Management standards/procedures CITD-0020 and CITD-0021 to manage AD infrastructure changes and have developed an SOP to support the commissioning and decommissioning of domains/domain controllers, however an SOP to provide guidance and management over GPOs does not exist. SOPs are critical in providing direction to the team members for the steps and procedures to follow while performing day to day responsibilities. Without proper governance in place there is lack of accountability and ownership for problem resolution resulting in adverse service delivery.	IA recommends Active Directory team formalize the existing SOPs by adding information regarding relevant stakeholders, document owner, revision history and evidence of sign offs and document guidance around managing GPOs. Additionally, IA recommends creation of a new SOP document with steps and procedures to follow while managing and handling support calls when an event / outage is identified	

Remaining Project Schedule

Project Schedule			
Step	Description	Expected Date	Status
1	**Phase I – Planning and Scoping** Kick Off Meeting	November 2021	Completed
2	**Phase II – Control Analysis** Walkthrough Interviews & Control Validation	December 2021	Completed
3	**Phase III – Fieldwork and Testing** Data Analysis & Test Execution	January 2022	In Progress
4	**Phase IV – Reporting** Audit Report	February 2022	In Progress

Appendix

Engagement Details

Objectives & Inherent Risks

Objective Area	Related Inherent Risk*	Key Areas of Focus
AD Management	AD infrastructure is not managed effectively which could result in lack of accountability and ownership for problem resolution resulting in adverse service delivery.	• Policies and Procedures which cover AD management processes • Clearly defined roles and responsibilities for AD administration • Management reporting of problems, changes, incidents etc.
Secure AD Boundaries	AD boundaries are not clearly defined which may lack security controls and may introduction vulnerability threats.	• Review AD design and structure (i.e. Domains, Trees, Forests, Organizational Units (OU)) • Review Segregation of Duties exists for critical AD functions like Administration, Monitoring, Making Changes etc. • Review Domain Trusts relationship
Secure Domain Controllers	Failure to secure the enterprise Domain Controllers may result in exposure to security threats through unauthorized system access.	• Review documented AD Domain Controller installation procedures and processes • Availability of Domain Controllers • Regular updates of Service Packs • Change management procedures associated with AD configurations settings which include Group Policy Objects (GPO) and Organizational Unit management

***Reflects the level of risk that exists in the absence of controls**

Note: *While the audit will focus on the objectives listed above, IA has a responsibility to assess any additional risks identified during the audit, and report any issues identified. Where applicable, issues will also be evaluated against requirements for Sarbanes-Oxley or other regulatory standards.*

Engagement Details

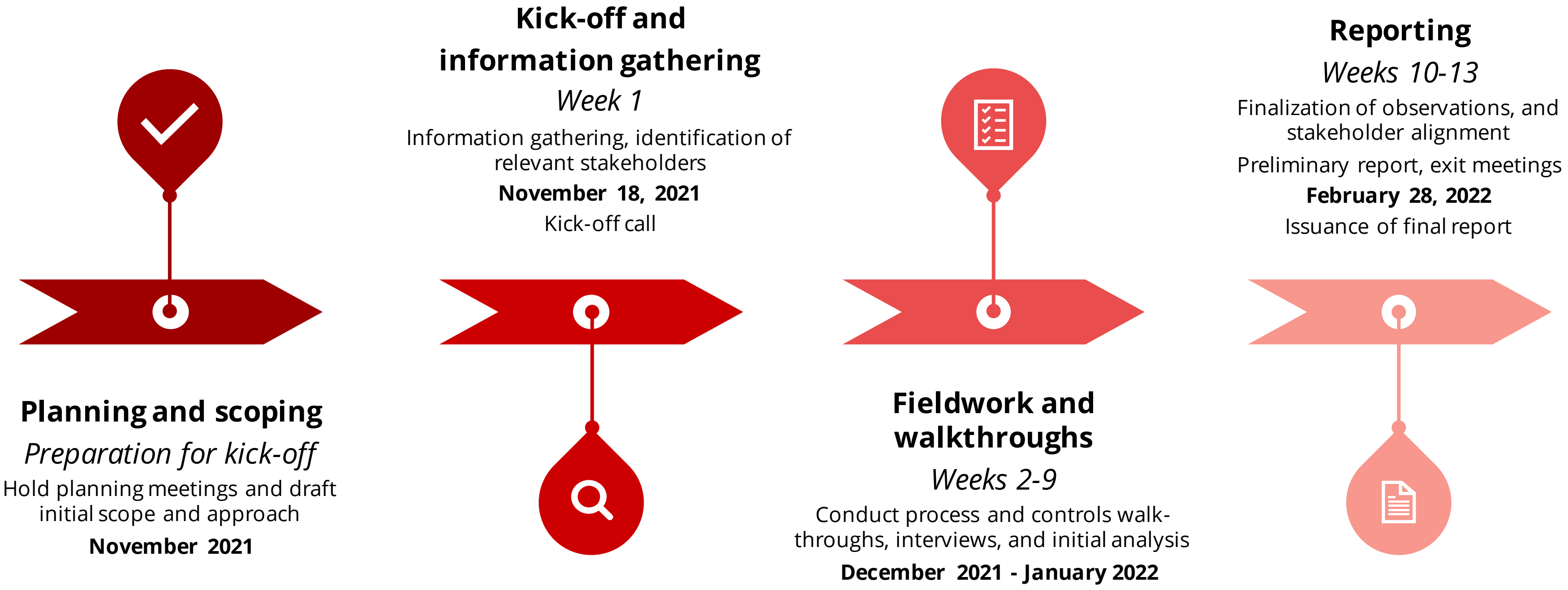
Objectives & Inherent Risks

Objective Area	Related Inherent Risk*	Key Areas of Focus
AD Administrative Practices	Administrative practices are not consistently followed which may impact AD operations.	• Administrator Account Limitations are based on job responsibilities. • Separate accounts for administrative and non-administrative operations
Logging and Monitoring	Logging settings not aligned with company requirements may result in critical AD operation activities not captured for management review.	• Evaluate AD Domain Controller Policy and Procedure requirements related to event, activity, logging and review • Review AD Domain Controller Monitoring activities for completeness

***Reflects the level of risk that exists in the absence of controls**

Note: *While the audit will focus on the objectives listed above, IA has a responsibility to assess any additional risks identified during the audit, and report any issues identified. Where applicable, issues will also be evaluated against requirements for Sarbanes-Oxley or other regulatory standards.*

Audit Timeline



Planning and scoping

Preparation for kick-off

Hold planning meetings and draft initial scope and approach

November 2021

Kick-off and information gathering

Week 1

Information gathering, identification of relevant stakeholders

November 18, 2021

Kick-off call

Fieldwork and walkthroughs

Weeks 2-9

Conduct process and controls walk-throughs, interviews, and initial analysis

December 2021 - January 2022

Reporting

Weeks 10-13

Finalization of observations, and stakeholder alignment

Preliminary report, exit meetings

February 28, 2022

Issuance of final report