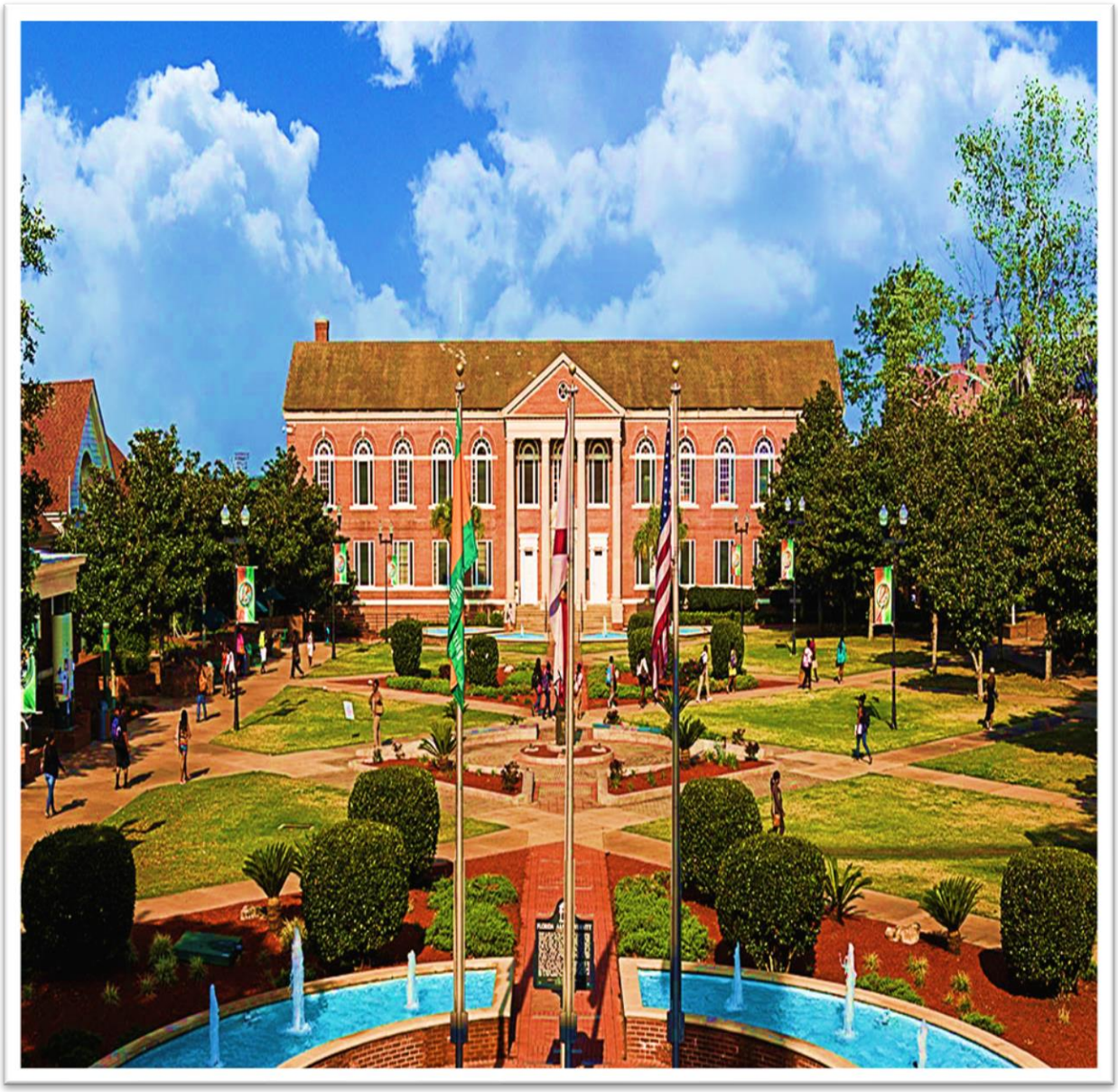
FLORIDA A&M UNIVERSITY
DIVISION OF AUDIT

Active Directory Security and Management Audit
Report: 20-21-0001
Audit Report



ACCOUNTABILITY ● INTEGRITY ● EFFICIENCY

November 30, 2020

Assurance Service 20-21-0001

EXECUTIVE SUMMARY

WHAT WE DID

In accordance with Division of Audit's Annual Work Plan approved by FAMU's Board of Trustees, we reviewed University Information Technology Services' (ITS) procedures and controls for securing the Windows Active Directory environment. We benchmarked the ITS' procedures and controls against industry leading practices and Microsoft's recommended controls to identify areas for improvements. The main areas we reviewed include the following[1]:

- Administrator account management;
- User account management;
- Security events monitoring;
- Password policy settings;
- Domain security policy setting;
- Audit policy setting;
- Active Directory security assessment; and
- Domain controller disaster recovery and data backup.

WHAT WE FOUND

We evaluated eight main Active Directory control areas summarized on the following pages and determined that five of the eight control areas tested need improvement and, without mitigating steps, present a high level of risk to the University.

Control Objectives	Control Summary	Control Assessment
Administrator accounts are granted based on roles and responsibilities, and account activities are monitored.	Lack of processes to routinely manage Active Directory domain Administrator accounts and monitor account activities.	**Needs Improvement**
Inactive or unused user accounts are timely disabled.	Inactive or unused Active Directory user accounts were not timely disabled.	**Needs Improvement**
Security events are actively monitored, mitigated, and reported to management.	ITS routinely monitored security events and security incidents were timely resolved	**Satisfactory**

[1] Domain controller physical security was part of the original audit scope but was removed due to health and safety protocols implemented by the University during the COVID-19 pandemic.

Control Objectives	Control Summary	Control Assessment
	and reported to management via real time alert notifications.	
Strong password policy is implemented.	The University was transitioning University departments into DUO Security[2], a two-factor authentication process for more secured sign on to University applications such as iRattler, Dropbox, DocuSign, and Zoom. The password policy for those departments who had not been transitioned to DUO was in alignment with industry best practices.	**Satisfactory**
Domain security policy settings are configured to identify and mitigate security threats.	Domain security policy settings were routinely monitored and configured to identify and mitigate security threats.	**Satisfactory**
Audit policy settings are configured to log security events for review and monitoring to facilitate risk-based decision making.	Audit policy settings were not properly configured to audit certain security events.	**Needs Improvement**
Domain Controller disaster recovery plan is developed and tested and full domain backup is performed regularly.	Full domain controller backups were not routinely performed. ITS did not have a documented disaster recovery plan to restore domain controllers in the event of incidents and the restore process had not been tested at the time of audit review.	**Needs Improvement**
Active Directory security assessment is performed regularly to identify and mitigate system deficiencies and vulnerabilities.	ITS lacked a comprehensive Active Directory security assessment to identify and remediate vulnerabilities and threats.	**Needs Improvement**

[2] Duo Security Inc. provides security software products and services. The Company provides authentication-as-a-service solutions, which leverages users' mobile phones as a second factor of authentication.

OPPORTUNITIES FOR IMPROVEMENT

During the audit, we found a number of key controls that were not in place or needed improvement. We recommend the Chief Information Officer take the following actions:

1. Develop a formal process for granting, modifying, and removing Active Directory administrator account access. Establish procedures for regular recertification of administrator account access and monitor activities of those accounts.

2. Perform regular cleanups of inactive or unused Active Directory user accounts in all Organizational Units (OUs).

3. Configure domain audit policy settings according to University's acceptable security risks and operational requirements and regularly review and update the configurations.

4. Perform regular full domain controller backups. Develop a written disaster recovery plan and test domain controller data backup restore process.

5. Perform routine vulnerability scans and comprehensive Active Directory security posture analysis to identify and mitigate any risks and vulnerabilities.

TABLE OF CONTENTS

BACKGROUND

Active Directory is a Microsoft directory service for Windows that provides mission-critical authentication, authorization, and configuration capabilities to manage users, computers, servers, and applications throughout an organization's IT infrastructure.

As of June 2020, FAMU's Active Directory was a single domain model with no applications connected to the University's domain required to have a trust relationship or subnetwork. Some primary applications' authentication controlled by Active Directory at FAMU include the Microsoft Office 365 suite of products, iRattler, ImageNow, and other select applications.

SATISFACTORY CONTROL SUMMARY

We compared ITS' security controls and procedures with those outlined in the *National Institute of Standards and Technology (NIST)* Special Publication 800-171[3] and 800-53[4], Microsoft Windows Active Directory control recommendations, and industry best practices. We determined that the controls listed in the table below and implemented by ITS are working effectively within the Active Directory environment.

Control Objectives	FAMU ITS' Control Highlights
Security events are actively monitored, mitigated, and reported to management.	ITS routinely monitored security events and incidents through automated software to identify incidents such as: • Failed password attempts; • User logins from another country; • Activity from anonymous proxy; • Impossible travel (e.g., a user logs in from a location where it would have been impossible for the user to travel to within a given time); and • Suspicious mailbox manipulation rules. Real time alert notifications of those events were emailed to management and ITS' Server Team. As an additional control, the Server Team regularly ran security event logs to identify these types of incidents. The Server Team performed procedures including immediate account lockouts and account removals to resolve identified incidents.
Strong password policy is implemented.	All Active Directory accounts must have passwords that adhere to the following criteria which were generally in line with

[3] *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
[4] *Security and Privacy Controls for Information Systems and Organizations*

Control Objectives	FAMU ITS' Control Highlights
	Microsoft's recommended password policy and complexity protocols which includes that passwords: • Must be at least 8 characters long; • Must contain at least one uppercase and one lowercase letter; • Must contain at least one special character or one number; • May not be any of the previous 5 passwords; and • Expires in 180 days. ITS is in the process of transitioning University departments into DUO Security, a two-factor authentication process for more secured sign on to University applications such as iRattler, Dropbox, DocuSign, and Zoom. ITS changed the password age from 90 days to 180 days after the remote work beginning March 18, 2020, due to COVID-19 to lessen the burden of password management for both users and ITS. This change does increase the risk of exposure for accounts not transitioned to Duo Security.
Domain security policy settings are configured to identify and mitigate security threats.	Key domain security policy settings shown below were configured according to Microsoft recommended settings: • Password Policy Setting; and • Account Lockout Policy.

OBSERVATION SUMMARY

Improvements are needed for the areas described below. The observation details and recommendations are included in the next sections.

Observation	Description	Owner	Risk Level	Remediation Deadline
Observation 1	Active Directory Domain Administrator Account	Chief Information Officer	High	1/1/2021
Observation 2	Active Directory User Account Cleanup	Chief Information Officer	Low	12/1/2020
Observation 3	Audit Policy Setting	Chief Information Officer	High	1/1/2021
Observation 4	Domain Controller Backup and Disaster Recovery	Chief Information Officer	High	2/1/2021
Observation 5	Active Directory Overall Security Assessment	Chief Information Officer	High	2/1/2021

OBSERVATION DETAILS

Observation 1 – Active Directory Domain Administrator Account

National Institute of Standards and Technology (NIST), Special Publication 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Section 3.1.5 requires organizations to "employ the principle of least privilege, including for specific security functions and privileged accounts. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions." Additionally, *NIST, Special Publication 800-53, Revision 5,* *Security and Privacy Controls for Information Systems and Organizations*, Section AC-2 Account Management, provides detailed control guidance on establishing, administering, and monitoring user access and user activities.

Active Directory domain administrator accounts are the most privileged accounts with full access (full control permissions) of the files, directories, services, and other resources on servers. Administrator accounts can be used to create local users, assign user rights and access control permissions. Therefore, those accounts should only be granted to individuals who need the access to perform their job duties. As of May 29, 2020, 19 administrator accounts were in active status. Of the 19 accounts, all but one was needed for performance of assigned job duties. The one account that was no longer needed was disabled after our review. Other issues noted during our review of administrator account management included**:**

a. ITS did not have formal processes for adding, modifying, and removing administrator accounts;
b. User access was not recertified on a regular basis to determine whether the access is absolutely needed to perform duties; and
c. Account activities were not monitored and managed.

Misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities may compromise system accounts and can have significant adverse impacts on the University. As a result, the risk level of this item is **High**.

Recommendation: The Chief Information Officer should direct staff to develop procedures and standards to strengthen controls related to domain administrator user accounts. The procedures and standards should address the following items:

a. Process for granting, modifying, and removing domain administrator account access;
b. Regular account recertification process; and
c. Monitoring of administrator account activities.

Observation 2 – Active Directory User Account Cleanup

NIST, Special Publication 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Section 3.1.5 requires organizations to "employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions." Additionally, *NIST, Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations*, Section AC-2 (3), Account Management states "disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality, which reduce the attack surface of the system. Specifically, disabling accounts that:

a. have expired;
b. are no longer associated with a user or individual;
c. are in violation of organizational policy; or
d. have been inactive for a set number of periods."

ITS Server Team staff is responsible for writing and running scripts to identify Active Directory account users, their account creation dates, and last logon dates for users in various Organizational Units (OUs) across the University, including Faculty, Staff, Incoming Students, and Applicants. ITS' process for user account cleanup is to disable inactive accounts after 120 days. We judgmentally selected user accounts in the "Incoming Students' OU for review as users in this group tend to have frequent changes. Our testing revealed that 840 of 1,665 user accounts were never used to log into the system or had no activity for 120 days. However, users' access was not disabled as required.

The unused accounts residing in Active Directory increase the risk of unauthorized access to systems. While ITS does have process in place to disable inactive accounts, cleanup was not performed on a regular basis. However, due to student accounts having limited access to critical data, the risk level for this item is **Low**.

Recommendations: The Chief Information Officer should direct staff to:

1. Review the Active Directory user accounts in other OUs and make necessary account cleanups; and
2. Develop a process to regularly identify and clean up inactive and unused Active Directory user accounts in all OUs.

Observation 3 – Audit Policy Settings

National Institute of Standards and Technology (NIST), Special Publication 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Section 3.3.1 states "Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity." Audit policies, when configured, allow domain controllers to log these security events into the security event log channel for review and monitoring as often as needed to provide important information to organizations to facilitate risk-based decision making.

A Microsoft Windows audit policy defines the type of events that should be monitored in a Windows environment. It contains rules that define the limits of a policy and workflows to process violations after they occur. Audit scans use the criteria defined in an audit policy to evaluate whether violations have occurred in the organization. An auditing policy is an important detective control to review security incident logs to find outliers and patterns for violations.

Our review showed that ITS had not configured policy settings for the areas included below due to management's concern over slower processing after applying audit policy setting on servers.

- Account Logon
- Account Management
- Logon and Logoff
- Policy Change
- Privilege Use
- System

Missing audit policy settings increase the risk that accountability cannot be established for activities on the system. As a result, the risk level for this item is **High**.

Recommendations: The Chief Information Officer should direct staff to:

1. Configure domain audit policies in accordance with industry best practices and or Microsoft's recommended parameters based on University's acceptable security risks and operational requirements; and
2. Establish a formal process to regularly review and update the baseline configurations of the domain controllers.

Observation 4 – Domain Controller Backup and Disaster Recovery

National Institute of Standards and Technology (NIST), Special Publication 800-53, revision 5, Security and Privacy Controls for Information Systems and Organizations. The "Contingency Planning" section provides overall standards and guidelines around the area including criteria and controls related to Contingency Plan (CP-2), Contingency Plan Testing (CP-4), Alternate Storage Site (CP-6), Information System Backup (CP-9), System Recovery and Reconstitution (CP-10). The criteria address controls to keep an organization's critical functions operating in the event of disruptions.

ITS does not have a disaster recovery plan, in which, one of the key tasks is to restore data from backups to restore the Active Directory to a functional state in the potential event of a disaster or security incident. In the absence of a disaster recovery plan, ITS has a process to backup Domain Controllers. Our review shows that the last full backup for the four Domain Controllers was performed in July, 2019. And system state backups are performed weekly for components needed to restore the Active Directory. Our review disclosed several issues with the backups described below:

a. ITS did not have a process in place to perform routine full domain controller backup;
b. Backed up data were stored on a portable drive located onsite. While storing backups on a portable drive could be reliable and cost effective, placing the portable drive at the same location where the servers are located does not prevent the data from disaster or disruption that occurs at the same location; and
c. The restore process had not been tested to determine data can actually be recovered.

Not having a disaster recovery plan including adequate Active Directory domain controller backup process will increase risks of users losing administrative authority and loss of data in the event of a disaster or emergency. They may impact continuous University operations, result in reduction in production, financial loss, and reputational loss. Therefore, the risk level is **High**.

Recommendation: The Chief Information Officer should direct staff to:

1. Perform routine full domain controller backup for all server data, including applications and the operating system. ITS should place backup data at a safe offsite location other than where the servers are located; and
2. Develop a written disaster recovery plan to address at the minimum the following items:
    a. Roles and responsibilities of staff leading the Active Directory recovery efforts;
    b. Disaster scenarios, coordination of recovery efforts, and communication methods;
    c. Business impact of application failures and loss of data;
    d. Backup strategy for reference and transactional data; and
    e. Regular assessment and retesting of the recovery process.

Observation 5 – Overall Active Directory Security Assessment

National Institute of Standards and Technology (NIST), Special Publication 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Section 3.12 Security Assessment require organizations to "1) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application; 2) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems; and 3) Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls."

Management can achieve the objectives by implementing industry recommended approaches including:

1. **Vulnerability Scans:** Vulnerabilities are weaknesses in a system that may be leveraged by threat actors to adversely affect the confidentiality, integrity, or availability of the system or data. Vulnerability scanning helps identify outdated software versions, missing patches, and misconfigurations that open doors for security incidents. Vulnerability scanning helps correct the security weaknesses through system upgrades or patches, before they can be exploited.
2. **Microsoft 365 Secure Score:** According to Microsoft, the Microsoft Secure Score "is a numerical measurement of an organization's security performance based on system configurations, user behavior and other security related measurement." The Secure Score is calculated based on five categories comprised of Microsoft 365 identities, Data, Apps, Devices, and Infrastructure to assess the current state of the security posture. "The score represents the extent to which an organization has adopted security controls in the Microsoft environment which can help offset the risk of being breached." Based on the above assessment, Microsoft 365 Secure Score provides guidance and recommended actions to protect organizations from threats.

Our review determined that ITS did not regularly perform an overall assessment of its Active Directory security environment. Specifically, ITS had not performed vulnerability scans on all four domain controllers. In addition, the most recent Microsoft 365 Secure Score (Score) ran by ITS did not represent Active Directory security posture in its entirety since ITS does not use some criteria that are used to calculate the final score, therefore, the Score did not fully indicate the overall security status of the Active Directory environment.

Without a regular evaluation of overall security posture of the Active Directory, ITS is less likely to timely and effectively identify and remediate any vulnerabilities. The domain controllers are susceptible to potential cyberattacks, thus undermining the entire IT infrastructure. As a result, the risk level is **High**.

Recommendation: The Chief Information Officer should direct staff to establish a process to schedule regular vulnerability scans and comprehensive Active Directory security posture analysis to identify, monitor, and mitigate any risks and vulnerabilities.

APPENDICES

APPENDIX A – PURPOSE, SCOPE, AND METHODOLOGY

Purpose

The purpose of this audit was to:

- Evaluate technical security controls of Active Directory for alignment with best practices;
- Evaluate the University process for allowing systems to connect with active directory for compliance with risk management practices;
- Evaluate the effectiveness of active directory maintenance procedures; and
- Evaluate the active directory disaster recovery plan and testing schedule.

Scope

We evaluated the University's processes and procedures that address controls in the area of Active Directory. Our review generally focused on the following areas:

- Administrator account management;
- User account management;
- Security events monitoring;
- Password policy and complexity;
- Domain security policy setting;
- Audit policy setting;
- Overall Active Directory security assessment;
- Domain Controller disaster recovery and data backup; and
- Physical security of the Domain Controllers[5]

Methodology

To achieve the audit objectives we:

- Conducted questionnaires to gain understanding of the Active Directory maintenance and management;
- Detailed testing of selected transactions (data) to determine whether control procedures were performed and effective to ensure Active Directory security;
- Performed real time observation of selected configuration settings and scripts;
- Interviewed of key staff regarding processes and responsibilities for administering and securing Active Directory; and
- Compared University ITS procedures of managing Active Directory and ongoing monitoring with industry best practices including Microsoft's recommended controls and benchmarks.

[5] Physical security of domain controllers was part of the audit scope. However, DoA was not able to perform detailed testing as a result of moving to remote work beginning March 18, 2020, due to the COVID-19 pandemic.

APPENDIX B – CORRECTIVE ACTION PLAN

Issue	DoA Recommendations	Corrective Action Plan	Responsible Party & Implementation Date
1. Active Directory Domain Administrator Account As of May 29, 2020, nineteen (19) Administrator accounts were in active status. Of the 19 accounts, all but one was needed for performing duties and conducting projects. The one account that was no longer needed was disabled after our review. We also found issues included: a. ITS does not have formal processes for adding, modifying, and removing Administrator accounts. b. User access are not recertified on a regular basis to determine whether the access is absolutely needed to perform duties. c. Account activities are not monitored and managed.	ITS should develop procedures to strengthen controls related to domain Administrator user accounts. The procedures should address, at a minimum, the following items: a. Process for granting, modifying, and removing domain Administrator account access. b. Regular account recertification process. c. Monitoring of Administrator account activities.	1. Cleanup current Active Directory Administrator Accounts by removing any current Administrator Accounts that are no longer needed. 2. Include creating, recertifying, and removing Active Directory Administrator Accounts in the process and procedures developed as part of the Access Control standards being developed and implemented in order to improve compliance with NIST 800-171. 3. Include monitoring of Administrator Account activity in the process and procedures developed as part of the Audit and Accountability standards being developed and implemented in order to improve compliance with NIST 800-171.	Responsible Party: **Ronald Henry** Implementation Date: **10/1/2020** Next Review Date: **12/1/2020** Next Review Date: **1/1/2021**

Issue	DoA Recommendations	Corrective Action Plan	Responsible Party & Implementation Date
2. Active Directory User Account Cleanup ITS' process for user account cleanup is to disable inactive accounts after 120 days for users in various Organizational Units (OUs), including Faculty, Staff, Incoming Students, and Applicants. We judgmentally selected user accounts in the "Incoming Students' OU for review. Our testing revealed that 840 of 1,665 user accounts had never logged into the system or had no activities after 120 days. However, the user access was not disabled at the time as required.	1. ITS should review the Active Directory user accounts in other OUs and make necessary account cleanups. 2. ITS should develop a process to regularly identify and clean up inactive and unused Active Directory user accounts in all OUs.	**1.** Work with applicable colleges, schools, and division to identify inactive and unused user accounts in order to cleanup current Active Directory User Accounts. **2.** Include regular Active Directory cleanup procedures in the process and procedures developed as part of the Access Control standards being developed and implemented in order to improve compliance with NIST 800-171.	Responsible Party: **Ronald Henry** Implementation Date: **11/1/2020** Next Review Date: **12/1/2020**
3. Audit Policy Setting: A Microsoft Windows audit policy defines type of events should be monitored in a Windows environment and logs the events for review when auditing is turned on. An auditing policy is an important control for maintaining security and detecting security incidents. Our review identified	1. ITS should configure domain audit policies according to industry best practices and or Microsoft recommended parameters based on University's acceptable security risks and operational requirements. 2. ITS should establish a formal process to regularly	1. Work with the Microsoft Premier Support Team to define and configure the Windows audit policy in order to provide regular on-going audit logs for the identified key areas. 2. Include formal Active Directory audit procedures in the process and procedures	Responsible Party: **Ronald Henry** Implementation Date: **11/1/2020** Next Review Date: **1/1/2021**

Issue	DoA Recommendations	Corrective Action Plan	Responsible Party & Implementation Date
that ITS has not configured policy settings for key areas included: • Account Logon • Account Management • Logon and Logoff • Policy Change • Privilege Use • System Missing audit policy settings increase the risk that accountability cannot be established for activities on the system.	review and update the baseline configurations of the domain controllers.	developed as part of the Audit and Accountability standards being developed and implemented in order to improve compliance with NIST 800-171.	
4. Domain Controller Backup and Disaster Recovery ITS does not have a disaster recovery plan, in which, one of the key tasks is to restore data from backups to restore the Active Directory to a functional state in the potential event of a disaster or security incident. In the absence of a disaster recovery plan, ITS has a process to backup Domain Controllers.	1. ITS should perform routine full domain controller backup for all server data, including applications and the operating system. ITS should place backup data at a safe offsite location other than where the servers are located. 2. ITS should develop a written disaster recovery plan to address:	1. Complete full domain controller backup to be stored both on-site and an off-site location. 2. Develop and implement a schedule for routine full domain controller backup to be stored both on-site and an off-site location. 3. Include regular Domain controller backup procedures	Responsible Party: **Ronald Henry** Implementation Date: **12/1/2020** Implementation Date: **12/1/2020**

Issue	DoA Recommendations	Corrective Action Plan	Responsible Party & Implementation Date
Our review shows that the last full backup for the four Domain Controllers was performed in July, 2019. And system state backups are performed weekly for components needed to restore the Active Directory. Our review disclosed several issues with the backups described below: a. ITS does not have a process in place to perform routine full domain controller backup. b. Backed up data is stored on a portable drive located onsite. While storing backups on a portable drive could be reliable and cost effective, the portable drive placed at the same location where the servers are located does not prevent the data from disaster or disruption	a. Roles and responsibilities of staff leading the Active Directory recovery efforts. b. Disaster scenarios, coordination of recovery efforts, communication methods c. Business impact of application failures and loss of data. d. Backup strategy for reference and transactional data. e. Regular assessment and retesting of the recovery process.	in the process and procedures developed as part of the Contingency Planning standards being developed and implemented in order to improve compliance with NIST 800-53. 4. Include written Disaster Recovery plan in the process and procedures developed as part of the Contingency Planning standards being developed and implemented in order to improve compliance with NIST 800-53.	Next Review Date: **2/1/2021** Implementation Date: **2/1/2021**

Issue	DoA Recommendations	Corrective Action Plan	Responsible Party & Implementation Date
occurs at the same location. c. The restore process has not been tested to determine data can actually be recovered.			
5. Overall Active Directory Security Assessment ITS does not regularly perform overall assessment of its Active Directory security environment. Specifically, ITS has yet performed any vulnerability scans on all four domain controllers. In addition, the most recent Microsoft 365 Secure Score (Score) ran by ITS did not represent Active Directory security posture in its entirety since ITS does not use some criteria that are used to calculate the final score, and thus, the Score did not fully indicate the overall security status of the Active Directory environment.	ITS should establish a process to schedule regular vulnerability scans and comprehensive Active Directory security posture analysis to identify and mitigate any risks and vulnerabilities.	1. Complete full Active Directory Vulnerability Scan. 2. Develop and implement a schedule for routine Active Directory Vulnerability Scans. **3.** Include regular Active Directory Vulnerability Scans in the process and procedures developed as part of the Risk Assessment standards being developed and implemented in order to improve compliance with NIST 800-171.	Responsible Party: **Ronald Henry** Implementation Date**:** **11/1/2020** Implementation Date**:** **11/1/2020** Implementation Date**:** **2/1/2021**

DISTRIBUTION

Responsible Managers:

- Ronald Henry, Associate Vice President & Chief Information Officer, ITS

Internal Distribution:

- Board of Trustees
  - Kelvin Lawson, Chair
  - Kimberly Moore, Vice Chair
  - Craig Reed, Audit and Compliance Committee Chair
  - Ann Marie Cavazos
  - Thomas W. Dortch, Jr.
  - Kristin Harper
  - David Lawrence, Jr.
  - Xavier McClinton
  - Belvin Perry, Jr.
  - Kenward Stone
  - Nicole Washington
  - Robert L. Woody
- FAMU Executive Leadership Team
  - Larry Robinson, Ph.D., President
  - Denise Wallace, Vice President, Legal Affairs and General Counsel
  - Maurice Edington, Provost and Vice President, Academic Affairs
  - Alan Robertson, Vice President, Finance and Administration/CFO

External Distribution:

Julie Leftheris, Inspector General and Director of Compliance, Board of Governors

PROJECT TEAM

Engagement was conducted by:
Ruoxu Li, CIA, CISA
Senior IT & Data Analytics Auditor

Engagement was supervised by:
Deidre Melton, CFE, CIA, CISA, CISM, CRISC
Audit Director

Engagement was approved and distributed by:
Joseph K. Maleszewski, MBA, CIA, CGAP, CISA, CIG, CIGA, CIGI, CCEP
Vice President for Audit

STATEMENT OF ACCORDANCE

The Division of Audit's mission is to provide independent, objective assurance and consulting services designed to add value and improve the University's operations. It helps the University accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

We conducted this assurance service in accordance with the International Standards for the Professional Practice of Internal Auditing, the Generally Accepted Government Auditing Standards, and the *Information Systems Auditing Standards* published by ISACA. Those standards require we plan and perform the assurance service to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our engagement objectives. We believe the evidence obtained provides a reasonable basis for our conclusions based on our objectives.

Please address inquiries regarding this report to the Division of Audit at (850) 412-5479.

http://www.famu.edu/index.cfm?AuditandCompliance&AboutAuditandCompliance