OBM | Office of Internal Audit

Department of Natural Resources
Access Controls Audit

Audit Period: October through December 2018

Results Summary:

Objective	Conclusion
Evaluate the effectiveness of user access and security controls over agency's Windows Active Directory.	**Improvement needed**

* Refer to Appendix A for classification of audit objective conclusions.

Report number: 2019-DNR-20 **Issuance date: December 13, 2018**

Executive Summary

Background

The Ohio Department of Natural Resources (DNR) is charged with overseeing the use, preservation, and conservation of the State's natural resources through a wide variety of recreational and regulatory programs. DNR's areas of responsibility include Ohio's wildlife, forests and other natural areas, state parks, inland lakes and waterways, geological and mineral resources, and the Lake Erie coastline. The Department consists of ten operating divisions and offices that carry out these functions, as well as central administrative offices that oversee the day-to-day functions of the Department. DNR's programs are divided into the divisions of Forestry, Parks and Watercraft, Water Resources, Natural Areas and Preserves, Wildlife, Geological Survey, Mineral Resources Management (DMRM), Oil and Gas Resources Management, Engineering, and the Office of Coastal Management.

The OBM Office of Internal Audit (OIA) conducted a review of access controls for DNR's Active Directory to determine the adequacy of the internal control environment, including assurance testing of the controls.

During the audit, OIA identified opportunities for DNR to strengthen internal controls and improve business operations. A summary, along with detailed observations, has been provided. OIA would like to thank DNR staff and management for their cooperation and time in support of this audit.

This report is solely intended for the information and use of agency management and the State Audit Committee. It is not intended for anyone other than these specified parties.

Scope and Objectives

OIA staff was engaged to perform an assurance audit related to the controls over the agency's access control process. This work was completed October through December 2018. The objective of this audit is as follows:

- Evaluate the effectiveness of user access and security controls over agency's Windows Active Directory.

The detailed scope of the engagement is as follows:

- Review access controls of all active Domain Controllers.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. Low risk observations were discussed with individual agency management and are not part of this report. However, the low risk observations were considered as part of the audit objective conclusions.

Observation 1 – Password for privileged accounts set to never expire

DAS Policy, ITS-SEC-02, states NIST Special Publication 800-53 is the framework for information security control implementation for the state. NIST 800-53 IA-5 Authenticator Management states "The organization manages information system authenticators by:

- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];

OIA evaluated a complete population of the Active Directory privileged accounts and noted the following access control errors:

- The password for one (1) Enterprise Administrator account was set to never expire.
- The password for eight (8) service accounts was set to never expire.

The current password policy does not address the requirement for management to perform periodic reviews to ensure password settings are appropriate. Failure to ensure security standards for password management are enforced increases the risk those accounts could be used to gain unauthorized access to and manipulation of resources with sensitive data.

Recommendation

All accounts at DNR should be set to expire. The service accounts should be set to expire within a year and a service account password renewal step should be performed as part of the annual system maintenance process. The password policy should be updated to include a process to review password management data within the Active Directory domain on a regular basis. This will provide assurance that account password settings align with the agency policy and/or industry best practices, including expiration of an account in an appropriate timeframe, unless

approved by management for reasonable justification. Management should utilize NIST SP800-53 for guidance on the requirements that should be implemented into the policy.

Management Response

All accounts at DNR shall be set to expire. The service accounts will be set to expire within one year and the service account renewal will become a documented annual process.

DNR will provide the following documentation as evidence of remediation:

- DNR will update the Password Pin Policy to include review for password management.
- DNR will create a written procedure for password review.
- DNR will provide screenshots of the remediation of the 9 accounts referenced above referencing password expiration dates.

Risk*	Remediation Owner	Estimated Completion Date
High	Jeff Rowley, IT Project Manager	January 31, 2019

Observation 2 – Terminated user access is not removed or modified in a timely manner

DAS Policy, ITS-SEC-02, states NIST Special Publication 800-53 is the framework for information security control implementation for the State. NIST 800-53, rev. 4, PS-4 Personnel Termination states "the agency, upon termination of individual employment, disables access by the end of the user's last business day and terminates/revokes any authenticators/ credentials associated with the individual."

The Department of Natural Resources has a formal Information Security Framework Policy. The policy states that DNR shall "establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor."

OIA reviewed the Active Directory data extract, the current OAKS DNR Active user listing, and OAKS Separated user listing for the period 1/1/2018 – 11/7/2018.

The following exceptions were noted during the test:

- Fifty (50) enabled network accounts were not included in the DNR OAKS Active Employees file.

- Twelve (12) of the fifty (50) accounts were included in the DNR OAKS Separated Employees listing.

- Thirty-eight (38) of the fifty (50) accounts were not included in the DNR OAKS Active employees file nor in the DNR OAKS Separated Employees listing.

The Department of Natural Resources' process requires the various Human Resources Divisions/Offices to send IT authorization to remove employees from the system. This process is manual in nature and the accounts may inadvertently be missed. The failure to disable user accounts after separation in a timely manner increases the risk of unauthorized access to systems and data, attacks on systems, and loss of accountability.

Recommendation

All "Enabled" terminated user accounts should be "Disabled" in a timely manner. Management should consider implementing a verification process that validates all terminated users have been actually removed or modified after the user reconciliation process is completed. Also, management should investigate and eliminate the reasons causing these accounts to be missed.

Management Response

All DNR active directory accounts are disabled by an automated process that triggers when Human Resources terminates an employee in OAKS. DNR and DAS created an automated process in December of 2017 for disabling accounts to the DNR-AD system. This currently ensures that DNR can disable all DNR accounts within 3 hours of the termination entry into OAKS.

DNR will onboard and offboard 500-600 seasonal employees annually. During the current audit, the active employee extract (Provided by the Office of Human Resources) and the AD extract (Provided by the Office of Information Technology) were run 4 days apart during a heavy offboarding period.

The gap produced the results described above. In addition, it is a common practice for Human Resources to back-date the termination which will result in a discrepancy in the date the employee was terminated and the date the employee was disabled in active directory when in fact the employee was disabled within 3 hours of the termination entry in OAKS.

DNR performs a quarterly audit to ensure that the automated process is working properly. The audit is outlined in the *User Active Directory and Computer Room Access Reconciliation Procedure.*

DNR will perform the following remediation steps:

- Self-Audit - DNR will regenerate the original extracts to identify the proper order in which the information should be produced to eliminate gaps and produce proper results for future auditing.

- DNR will identify instances where terminations are back dated and seek to create a report in OAKS to identify entry time and date to compare with accounts disabled date and time in DNR-AD. DNR will review this report as part of the Quarterly Audit to ensure that accounts are being disabled in a timely manner.
- DNR will modify *User Active Directory and Computer Room Access Reconciliation Procedure* to reflect review process changes to include the review for timeliness.
- DNR will share results with OIA and provide updated procedure.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	Jeff Rowley, IT Project Manager	March 31, 2019

Observation 3 – Lack of privileged account periodic review

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standard, AC-2 Account Management, states that agencies should require accounts with elevated privileges to "specify authorized users of the system and ensure required approvals for requests to create accounts." The agency should manage "creating, enabling, modifying, disabling, and removing accounts (including adding and deleting members from groups or roles)."

Through review, we noted that DNR has a process in place for approving system access to employees. However, OIA identified that twenty-eight (28) accounts with elevated privileges do not have documented approvals and justification credentials.

The failure to periodically verify that these accounts are appropriate and required increases the risk to the confidentiality, integrity, and availability of systems and data.

Recommendation

Management should follow the approval process by submitting the access approval form for employees who need system access. The process can be automated using a ticketing system. Further, Management should perform a periodic review process to verify that privileged accounts are granted with the appropriate access.

Management Response

DNR has an automated process in place for employees to request elevated privileges for workstations and servers. However, we don't use this process for employees who are part of our internal technical staff because support staff maintain a privileged account that has elevated

privileges. For tracking purposes, we are going create an automated request form for tracking elevated privileges for Office of Information support staff.

DNR will perform the following remediation steps:

- DNR will create an automated form for IT internal staff to document privileged access accounts.
- DNR will create and document a review process for auditing privileged access quarterly (This will require a modification to our current ServiceNow implementation to accommodate an electronic form to request and track this specific access).

Risk*	Remediation Owner	Estimated Completion Date
Moderate	Jeff Rowley, IT Project Manager	March 31, 2019

Observation 4 – Lack of a detailed log review process

DAS Policy, ITS-SEC-02, states NIST Special Publication 800-53 is the framework for information security control implementation for the State. NIST 800-53, rev. 4, AU-1 Audit and Accountability Policy and Procedures states "The agency should develop, document, and disseminate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls." Also, NIST 800-53, rev. 4, AU-6 Audit Review, Analysis and Reporting states that "The agency should review and analyze information system audit records on organization-defined frequency for indications of organization-defined inappropriate or unusual activity]; and reports findings to the agency personnel or roles".

OIA reviewed the Failed Login Report Review Procedures. It was noted that the document included steps for reviewing failed login attempts; however, it does not include some critical elements of the log review process, such as how to detect other suspicious activities, who will be performing the review, the frequency of the review, the tools that will be used to perform the review, and the escalation process for issues identified.

The lack of a detailed log review process increases the risk of unauthorized access to systems and data, attacks on systems, and loss of accountability.

Recommendation
Management should update the Failed Login Report Review Procedures to provide more detail. Providing elements such as how to detect other suspicious activities, who will be

performing the review, the frequency of the review, the tools that will be used to perform the review, and the escalation process for issues identified will enhance the log review process.		
Management Response		
DNR recognizes the need to update the Failed Login Report Review Procedure and will work with OIA to provide a satisfactory procedure. DNR will perform the following remediation steps: • DNR will modify the current Failed Login Report Review Procedures to provide the requested detail. • DNR will submit the modified Failed Login Report Review Procedures for approval.		
Risk*	**Remediation Owner**	**Estimated Completion Date**
Moderate	Jeff Rowley, IT Project Manager	January 31, 2019

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

Appendix A – Classification of Conclusions and Observations

Classification of Audit Objective Conclusions

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

Classification of Audit Observations

Rating	Description of Factors	Reporting Level
Low	Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.	Agency Management; State Audit Committee (Not reported)
Moderate	Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.	Agency Management and State Audit Committee
High	Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.	Agency Management and State Audit Committee