Neptune Enterprises External Audit Report on NIST SP 800-53 AC-2: Account Management

December 6th, 2024

Auditors: Connor Bressler, Cordell Rager, Jimmy St Cin

Contents

[Audit Scope 3](#_Toc183525758)

[Executive Summary 4](#_Toc183525759)

[Discovered Issues and Solutions 5](#_Toc183525760)

[Appendices 7](#_Toc183525761)

[Audit Procedure 7](#_Toc183525762)

[Fieldwork and Documentation 9](#_Toc183525763)

|  |
| --- |
| Audit Scope |
|  |

This audit is designed to ensure a focus on evaluating Neptune Enterprises’ systems and accounts and its adherence to the requirements outlined in NIST SP 800-53 for the AC-2 (Account Management) control. The auditing procedure assesses the policies, procedures and practices related to user accounts within Neptune Enterprises to ensure that they meet the security and operational requirements of the organization. Specifically, this audit will cover:

1. **Account Types:** Reviewing the types of accounts that are in use within Neptune Enterprises’ systems including accounts that have administrative privileges and just regular access.
2. **Account Managers:** Identifying members responsible for creating, modifying, deleting and managing accounts.
3. **Account Memberships:** Evaluating criteria and processes for assigning user accounts to specific groups or roles.
4. **Approval Processes for Accounts:** Assessing the procedures and employees responsible for authorizing account creation.
5. **Account Policies:** Reviewing policies for creating, enabling, modifying, disabling, and removing accounts.
6. **Account Monitoring:** Determining and evaluating if there are any tools that are used for monitoring account use (login times and file access) and sending notifications.
7. **Access Criteria for Information Systems:** Evaluating if there are any specific requirements (job responsibilities or the department an employee resides in) to decide system access
8. **Compliance Review:** Examining how accounts are reviewed for compliance with organizational policies and the frequency in which this is done.
9. **Shared/Group Accounts:** Evaluating how shared accounts with multiple employees are managed.
10. **Terminations and Transfers:** How the offboarding of accounts occurs.

|  |
| --- |
| Executive Summary |
|  |

Neptune Enterprises faces several account management challenges that pose significant security and compliance risks.

1. **Temporary Accounts Still Active**
   1. The audit identified an issue pertaining to part A of NIST SP 800-53 AC-2 (Account Management). Part A states that the types of accounts allowed and prohibited within Neptune Enterprises need to be documented and defined. This requirement is filled through Neptune Enterprises practices although, there is an issue pertaining to temporary accounts within systems. Temporary accounts within Neptune Enterprises’ systems remain active despite a claim that they were disabled. This issue exposes the organization to an increased risk in unauthorized access of accounts and exploitation risks.
2. **Documentation of Account Approval Process**
   1. The audit identified an issue pertaining to part E of NIST SP 800-53 AC-2 (Account Management). In part E, it states that approvals are required by personnel for requests to create accounts. Now, Mark is the one who approves these accounts, but there is no documentation for this process. The account approval process has no formal documentation at all, and this can lead to accountability challenges and difficulty in monitoring accounts.
3. **Absence of Lifecycle Policy**
   1. The audit identified an issue pertaining to part F of NIST SP 800-53 AC-2 (Account Management). Part F states that accounts should be created, enabled, modified, disabled, and removed in accordance with organization defined policies and procedures. The issue at hand here is that Mark describes what he does when creating, modifying, or removing accounts, but it seems that these procedures are not clearly defined and documented within the organization. The absence of a lifecycle policy procedure results in inconsistent practices, increasing the chance of account mismanagement and errors in account creation, modification, and termination.
4. **No Process for Changing Group Account Passwords**
   1. The audit identified an issue pertaining to part K of NIST SP 800-53 AC-2 (Account Management). In part K, it states that there should be a process for changing shared or group account authenticators (passwords) when an individual leaves the group. Currently from what Mark said, there is no procedure in Neptune Enterprises to fulfill this requirement, not to mention that temporary accounts within Neptune Enterprises systems are not disabled, which is another separate issue. Having no process for updating shared account passwords when employees leave workgroups leaves the chance for them to be able to re-gain access to user accounts and other information systems, resulting in potential security issues.

|  |
| --- |
| Discovered Issues and Solutions |
|  |

**Issue 1:** Temporary accounts within Neptune Enterprises remain active and have valid passwords even though it was believed that these accounts were disabled. These temporary accounts are still active, and this is indicated by the absence of lock symbols or exclamation marks in the contents of the etc/shadow file.

**Issue 1 Risk:** Failing to disable or lock temporary accounts increases the risk for unauthorized access to occur and creates accountability issues. Ultimately, it allows for a greater chance for these accounts to be exploited to bypass standard security controls.

**Issue 1 Solution:** Implement a group account policy that requires the immediate disabling and removal of temporary accounts once they are no longer needed. This can be done through scripts to ensure compliance with this policy. Mark should be responsible for creating this policy, although, outsourcing it to an IT contracting company could be an option as well. Whether Mark does it, or he gets outside help, this policy should be fully operational within two weeks from the submission date of this audit which is December 6th.

**Issue 2:** Neptune Enterprises’ approval process for creating new accounts does not align with the requirements of NIST 800-53 AC-2 part E. In part E, it states that approvals are required by personnel for requests to create accounts. Now, Mark is the one who approves these accounts, but there is no documentation for this process. Mark’s account approval process lacks formal documentation and a structured workflow, making it difficult to track when new accounts are made and assigning accountability to those accounts.

**Issue 2 Risk:** Without proper documentation regarding the approval process and the attributes of the newly created account, this can lead toaccountability issues and potential confusion, miscommunication, and difficulty in monitoring and auditing account activity. Lack of documentation in the approval process may increase the risk of non-compliance within Neptune Enterprises.

**Issue 2 Solution:**

Implement a formal process that outlines how to provide detailed documentation for the creation of all new accounts. This formal process should document the purpose of the account being created, the group it is going to be added to, and the date it was created. Mark should then review and sign off on this process. Eventually, Harry and Mark should do this jointly for every account through dual authorization. This process should be implemented within a month from December 6th to establish clear accountability.

**Issue 3:** Neptune Enterprises’ process on creating, enabling, modifying, disabling and removing accounts within the organization does not align with the requirements of NIST SP 800-53 AC-2, part F. Part F states that accounts should be created, enabled, modified, disabled, and removed in accordance with organization defined policies and procedures. The issue at hand here is that Mark describes what he does when creating, modifying, or removing accounts, but it seems that these procedures are not clearly defined and documented within the organization. Essentially, there is no lifecycle policy in place to outline and document these procedures Mark does, which leaves a gap in future guidance for account management.

**Issue 3 Risk:** With no lifecycle policy, there is no accountability and consistency in the consistency of creating, enabling, modifying, disabling or removing accounts. Having no lifecycle policy can lead to error and delays when dealing with account management. Future employees who are managers of accounts may struggle to handle accounts effectively, increasing the risk of mismanagement.

**Issue 3 Solution:** Develop a clear lifecycle policy detailing procedures for creating, modifying, and disabling and removing user accounts. This policy should include steps, employees who are responsible for performing these steps, and a timeline for each stage of the account lifecycle. Mark should be responsible for creating this policy and it should be implemented within three months from December 6th to provide clear guidance when creating, enabling, modifying, disabling and removing accounts.

**Issue 4:** Neptune Enterprises’ process on changing group account passwords when an individual leaves the group does not align with NIST SP 800-53 AC-2, part K. In part K, it states that there should be a process for changing shared or group account authenticators (passwords) when an individual leaves the group. Currently from what Mark said, there is no procedure in Neptune Enterprises to fulfill this requirement, not to mention that temporary accounts within Neptune Enterprises systems are not disabled, which is another separate issue.

**Issue 4 Risk:** Without a process or organization defined requirement to change shared account passwords during employee offboarding, former employees may be able to re-gain access to user accounts and other information systems, resulting in potential security issues.

**Issue 4 Solution:** There should be an established process that needs to be in place to change shared account passwords whenever an employee exits a workgroup or leaves the company entirely. This process should be documented and performed by Mark and Mark should also be responsible for implementing this process within two months from December 6th to reduce risks with offboarded employees.

|  |
| --- |
| Appendices |
|  |

|  |
| --- |
| Audit Procedure |
|  |

Goal

Verify that account management practices for Neptune Enterprises’ accounts align with NIST SP 800-53 AC-2 requirements, ensuring secure, compliant, and effective handling of all user accounts.

Required Software, Tools and/or Documentation

1. NIST SP 800-53 AC-2 (Account Management) documentation
2. Standard Access to Neptune Enterprises’ server
3. Mark Smith’s contact information
4. Documentation regarding auditing questions to evaluate Neptune Enterprises’ account management practices and Mark Smith’s answer to those questions

Directions

1. Below are the questions that will be asked to evaluate Neptune Enterprises’ systems pertaining to NIST SP 800-53 AC-2. These questions will be asked by the auditor and answered by Mark Smith. Mark’s responses to these questions will be reported in the fieldwork documentation below along with whether or not Mark’s answers can be verified and any issues that arise.

**Auditing Questions to be asked by the auditor and answered by Mark Smith:**

1. We are looking to find out if Neptune Enterprises has different levels of accounts, such as administrative accounts with elevated privileges versus standard accounts that have just limited access.
   1. Does Neptune Enterprises also use any temporary or guest accounts for vendors or temporary employees? For this question we are really just looking to see if there are accounts within Neptune Enterprises that have more, or less administrative privileges based on the employee's role.
2. Who is responsible for managing user accounts within Neptune Enterprises?
   1. Is there someone responsible for creating, modifying, and disabling accounts?
3. Are there defined criteria for assigning an employee’s user account to specific groups or roles?
4. Is there an approval process for creating new accounts?
   1. If so, who is responsible for authorizing approvals for the creation of new accounts?
5. Are there defined procedures that are used for creating, enabling, modifying, disabling, and removing accounts from Neptune Enterprises’ systems?
6. Are there any tools or procedures that you use to track login times for user accounts or when users access specific files and applications?
   1. Are there any logging or alert systems or software in place to monitor these examples of accounts activity?
7. Are there any specific requirements such as job responsibilities or the department that an employee resides in that Neptune considers when deciding what type of access each user should have?
8. How often are user accounts reviewed for organizational compliance?
   1. Who coordinates this process?
9. If there are shared or group accounts within Neptune Enterprises, is there a process in place for changing authentication to those accounts when individuals are removed from the group?
10. Could you outline how procedures for managing accounts are integrated with termination and transfer processes of employees?

|  |
| --- |
| Fieldwork and Documentation |
| Auditor Information   | Auditor Number | Auditor Name | Date Audited | | --- | --- | --- | | 1 | Connor Bressler | 11/18/2024 |   **Auditing Questions, Mark’s Responses, and Arising Issues/Notes**   1. We are looking to find out if Neptune Enterprises has different levels of accounts, such as administrative accounts with elevated privileges versus standard accounts that have just limited access.   Response From Mark:  I think they are all regular user accounts.  When I need to create a new account, I use GUI and just use the default settings – I think this is just a standard user account.  I do not give the new user any special permissions.  When my IT consulting firm originally set-up the Neptune server, they gave me administrative privileges as I would be setting up new users and doing some basic administration on the system.  The consulting firm also set up an IT Guys account in case they needed to do some maintenance I cannot do.  I also have the root password to the Neptune server.  Issues/Notes: Seems to be a discrepancy between standard account and admin account. Mark has admin privileges but a standard user account. He must know the root password. Not so much an issue but needs to understand the difference between an administrative account and a standard user account but with knowledge of the root password.   * 1. Does Neptune Enterprises also use any temporary or guest accounts for vendors or temporary employees? For this question we are really just looking to see if there are accounts within Neptune Enterprises that have more, or less administrative privileges based on the employee's role.   Response From Mark:  There are two temporary accounts that I use when it gets busy at Neptune.  I sometimes hire temporary employees around the holidays.  The accounts are tempdistro and tempsales.  They are used for temporary employees that need access to the information related to the distribution of goods and the sales of the goods.  At this time, we are not very busy, and no one is using the accounts and they should be disabled.  These should also be regular user accounts and have no elevated permissions.  Issues/Notes: This can be confirmed within the system that there are temporary accounts. Although, I want to see if they are actually disabled, going to need the etc/shadow file for this.  11/21/24: Mark was asked to show the contents of the etc/shadow file to ensure these temporary accounts were disabled. The contents of the file are shown below:  Image preview  Issues/Notes: So, it seems to be that these temporary accounts are indeed still active and not disabled. The P’s circled in the picture means that these accounts still have passwords. If these passwords were disabled, they would have an “L” in front of them signifying they are locked. If there was an exclamation point where the two red lines are in the picture, that would also signify that the accounts are disabled, but they are not. |
| 1. Who is responsible for managing user accounts within Neptune Enterprises?   Response From Mark:  Neptune is a small organization.  The only managers are myself and the newly hired assistant manager Harry.  I have typically done everything in this regard, but am hoping the Harry will be able to help out in the near future.    Right now Harry is still learning about his various roles at Neptune – I want him to be able to do everything that I do.  At the moment, he is mostly learning the ropes of the sales aspects of Neptune.    Issues/Notes: This is an assigned account manager and meets the requirement of AC-2. Mark is the only user with administrative privileges, therefore, it seems appropriate that he can only manage user accounts.   * 1. Is there someone responsible for creating, modifying, and disabling accounts?   Response From Mark:  That has typically been my responsibility, but I hope that Harry can begin helping with this in the near future.  Issues/Notes: As said above, this is an assigned account manager who is the only user with administrative privileges, so this seems reasonable that he can only create, modify and disable accounts. |
| 1. Are there defined criteria for assigning an employee’s user account to specific groups or roles?   Response From Mark:  When I hire someone, they are hired for a specific purpose within Neptune. For example, Frank was hired to do sales; nothing else. So, I added him to the sales group and no other group. If I would later need him to assist with the distribution of goods in addition to his sales responsibilities, I would add him to the distribution group.  Issues/Notes: This does define the criteria required for group and role membership that is wanted in AC-2. If an employee is hired for a specific department, then they have access to that department’s resources only. Although, for better clarification for Harry and future employees, a possibly draft of a policy explaining this criteria would be helpful. |
| 1. Is there an approval process for creating new accounts?   Response From Mark:  When I hire a new employee that needs access to the Neptune system, I create an account for them.  Issues/Notes: This seems to be an issue. It seems that this is really an informal account approval process and there is no formal approval or documentation involved. Mark should provide documentation about the new accounts he creates such as who it is for, what group it resides in, and an official date of the account being approved and being created. Also, when Harry gets caught up to speed, this should require dual approval from Mark and Harry and they should both sign off on it.   * 1. If so, who is responsible for authorizing approvals for the creation of new accounts?   Response From Mark:  As the owner/manager of Neptune, I handle this task.  Issues/Notes: No issues with this, all seems reasonable. Can also be confirmed in the server as Mark is the only person to have administrative privileges to create accounts, therefore, he is the only one who can approve them. |
| 1. Are there defined procedures that are used for creating, enabling, modifying, disabling, and removing accounts from Neptune Enterprises’ systems?   Response From Mark:  Accounts are created via the graphical user interface on the server.  I access the User Accounts application and unlock the interface.  From there I create a standard account.  Other than myself and my newly hired assistant manager, there are no other administrators on the system.    Additionally, when I hire someone, they are hired for a specific purpose within Neptune. For example, Frank was hired to do sales; nothing else. So, I added him to the sales group and no other group. If I would need him to assist with the distribution of goods in addition to his sales responsibilities, I would add him to the distribution group.    I use the groups so that employees with similar job functions can share files more easily. That is, if Frank is working on a contract with a new company and he takes a vacation, I would have access (as I also do sales) to read the files related to this company.    I am quite careful with how I assign groups, and this system has worked fine in the past.  Modifications to accounts would occur when an employee’s role within Neptune changes.  They would be added to the group associated with their new role.    Once someone is terminated, or quits, we will need to fill the position quickly so we advertise.  Until I hired Harry, I would handle all hiring by myself, but Harry will also be involved in the hiring process in the future.    Since I am the one who handles the accounts, I will know when things need to be changed or modified.  Hopefully, Harry will be able to help with this soon.  Issues/Notes: This is a good start. Mark explains how he goes about this process. Although, he needs to create a lifecycle policy explaining procedures and practices that align with how a user account is created, modified, or disabled/removed. This is an issue as not providing a lifecycle policy provides no guidance for future employees who may need to manage accounts. |
| 1. Are there any tools or procedures that you use to track login times for user accounts or when users access specific files and applications?   Response From Mark:  I do not have any special tools to monitor and manage notifications.  I do know the consulting firm told me they were going to enable typical system logging so that they can help track down problems in the system – if that ever happens.  Issues/Notes: This seems reasonable. Although it needs to be checked if it is actually running. So there needs to be a confirmation that rsyslog is indeed running.  Getting some type of technology to notify people when accounts are no longer required and when user are terminated or transferred is not necessary. This is a small company; Mark is the only one who makes decisions regarding managing accounts; therefore, he does not need to notify anyone else.  11/21/24: Mark was asked to show if rsyslog was running to confirm that there is some system logging going on to monitor account use. The picture he sent back that is below confirms that system logging is active for all Neptune Enterprises’ accounts. |
| A screenshot of a computer  Description automatically generated  Issues/Notes: It is good that there is system logging going on. This aligns with the AC-2 requirement of monitoring usage of accounts. Although Mark needs to show us the system log file to ensure that this is working correctly.  11/22/24: Mark was asked to show the log file for system logging to ensure that the system is logging user activity in real time. He sent a picture back showing the log file, it is below. Based on that picture, the system logging for accounts at Neptune Enterprises fulfills the requirement of AC-2 part G which is simply “monitoring the use of accounts”. |
| A screenshot of a computer  Description automatically generated   1. Are there any specific requirements such as job responsibilities or the department that an employee resides in that Neptune considers when deciding what type of access each user should have?   Response From Mark:  In general, there are four roles at Neptune – sales, distribution, catering and ordering.  The roles have responsibilities that you would expect.  For example, the sales role has to do with selling our product to customers, finding new customers and keeping them happy with Neptune.  Likewise, for the other roles.    When I hire someone, they are hired for a specific purpose within Neptune. For example, Frank was hired to do sales; nothing else. So, I added him to the sales group and no other group. If I would need him to assist with the distribution of goods in addition to his sales responsibilities, I would add him to the distribution group.    I use the groups so that employees with similar job functions can share files more easily. That is, if Frank is working on a contract with a new company and he takes a vacation, I would have access (as I also do sales) to read the files related to this company.  Issues/Notes: This fulfills the AC-2 requirement of authorizing access to a system based on valid access authorization, intended system usage, and other defined attributes. Mark makes an access authorization because he is the only one who can authorize use of accounts, then he grants that authorization based on the criteria of the employee being hired for sales or for another area of work. Employees are granted access based on what they hired for, that is considered a defined attribute and criteria. |
| 1. How often are user accounts reviewed for organizational compliance?   Response From Mark:  Review of user accounts occurs about once a year or when employees are hired, leave or change their role within Neptune.  Issues/Notes: This seems reasonable, although, if more employees are onboarded, reviewing accounts every six months may be necessary. No issues here.   * 1. Who coordinates this process?   Response From Mark:  Since I am the one who handles the accounts and employment, this would be my responsibility.  Issues/Notes: No issues here, only recommendation is that harry gets added to this process of reviewal when he catches up to speed.   1. If there are shared or group accounts within Neptune Enterprises, is there a process in place for changing authentication to those accounts when individuals are removed from the group?   Response From Mark:  I occasionally use shared accounts so that temporary employees can use common account when necessary.  At this time, we are not very busy so no one is using any of shared account and they should be disabled.  Issues/Notes: This is good practice, but there is an issue here. There needs to be a process that allows for a shared account password to be changed so when someone is removed from that group and the company, they cannot try and access it at a later time. Changing passwords of shared accounts when an employee leaves is a crucial part of the offboarding process. Also need to check the etc/shadow file.   1. Could you outline how procedures for managing accounts are integrated with termination and transfer processes of employees?   Response From Mark:  As the owner/manager of Neptune, I handle all employment issues.  I also manage accounts on the Neptune server.  As such, I will already know when someone is terminated or resigns.  Additionally, I know when employees transition from one position to another.  Issues/Notes: No issues here. Maybe provide documentation as to what processes are being used when terminating an employee or transferring them to another position. What did you do to accomplish the goal of removing or terminating an employee’s account. |