**Weekly Assignment 4**

Use this page as a guide <https://csf.tools/reference/nist-sp-800-53/r4/ac/ac-2/> and then answer the following questions about the page.

For each question you should provide a quarter page to half page length answer.

1. What do you think this page is about overall?

This page provides an overview of the "AC-2: Account Management" control from the NIST Special Publication 800-53, Revision 4, focusing on account management procedures and guidelines to support organizational missions and business functions.

• **Key Elements of AC-2: Account Management**

Control Statement

The organization is responsible for:

- Identifying and selecting types of information system accounts.

- Assigning account managers.

- Establishing conditions for group and role membership.

- Specifying authorized users and access authorizations for each account.

- Requiring approvals for creating accounts.

- Creating, enabling, modifying, disabling, and removing accounts according to procedures.

- Monitoring account usage.

- Notifying account managers about changes in account status (e.g., when accounts are no longer needed, users are terminated, or user needs change).

- Authorizing access based on valid authorization, intended system usage, and other required attributes.

- Reviewing accounts periodically for compliance.

- Reissuing shared/group account credentials when needed.

Supplemental Guidance

- Information system accounts include individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service accounts.

- Dynamic privilege management and role-based schemes should be implemented to manage account access.

- Conditions for disabling accounts include non-requirement of the account, user termination or transfer.

- Automated mechanisms for managing accounts are recommended for efficiency and security.

Control Enhancements

The enhancements to the basic control include:

- Automated account management.

- Removal or disabling of temporary/emergency accounts.

- Disabling inactive accounts automatically.

- Automated auditing of account actions.

- Enforcing inactive logouts.

- Implementing dynamic privilege management.

- Role-based access schemes.

- Dynamic account creation.

- Restrictions and credential termination for shared/group accounts.

- Monitoring and reporting atypical account usage.

- Disabling accounts for high-risk individuals.

Related Controls

Additional controls related to access enforcement, information flow, separation of duties, least privilege, concurrent sessions, remote access, mobile device access, use of external systems, audit information protection, and configuration management are also mentioned.

• **References**

The control aligns with various standards and guidelines including CSF v1.1, PF v1.0, Critical Security Controls, and Cloud Controls Matrix.

• **Threats Addressed**

Key threats addressed by these controls include spoofing, repudiation, and lateral movement.

• **Baselines**

Different baselines (Low, Moderate, High) define the specific implementations and requirements for each level of security control, ensuring tailored application based on organizational needs and risk profiles.

• **Transition to Revision 5**

NIST SP 800-53 Revision 5 introduces updates to these controls, maintaining the foundational requirements while integrating more advanced security practices and technological advancements.

1. What is the Control Statement section talking about?

The Control Statement section of AC-2: Account Management in NIST Special Publication 800-53, Revision 4, outlines the specific responsibilities and actions that an organization must undertake to manage information system accounts effectively. Here’s a detailed breakdown of each requirement:

**1. Identifies and selects account types**: The organization must determine the types of accounts needed (e.g., individual, shared, guest) to support its missions and business functions.

**2. Assigns account managers:** Designate personnel responsible for overseeing the management of these accounts.

**3. Establishes conditions for group and role membership:** Define the criteria for users to be part of specific groups or roles within the system.

**4. Specifies authorized users and access privileges:** Clearly identify who is authorized to use the system, what groups/roles they belong to, and their access privileges.

**5. Requires approval for account creation:** Implement a process where account creation requests must be approved by designated personnel or roles.

**6. Manages account lifecycle**: Ensure accounts are created, enabled, modified, disabled, and removed according to defined procedures and conditions.

**7. Monitors account usage**: Keep track of how accounts are being used to detect any unauthorized or unusual activity.

**8. Notifies account managers about changes**: Inform account managers when accounts are no longer needed, users are terminated or transferred, or when user roles change.

**9. Authorizes system access**: Grant access based on valid authorization, intended use of the system, and other required attributes.

**10. Reviews account compliance**: Regularly review accounts to ensure they comply with management requirements.

**11. Reissues shared/group account credentials**: Have a process in place to reissue credentials for shared or group accounts when members leave the group.

1. What is the Supplemental Guidance section talking about?

The Supplemental Guidance section provides additional details and context to help organizations implement the AC-2: Account Management control effectively. It elaborates on the key elements and considerations involved in managing information system accounts, offering practical advice and examples. Here’s a summary of what this section covers:

1. Types of Accounts: It lists various types of information system accounts, such as individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service accounts. This helps organizations recognize the diverse account types they may need to manage.

2. Implementation of Account Management Requirements: Some account management tasks can be automated using organizational information systems. For instance, the system might automatically monitor account usage or notify account managers of changes.

3. Authorization and Access Privileges: The process of identifying authorized users and specifying their access privileges must align with other security controls in the organization’s security plan. Administrative accounts, which require higher scrutiny, should be managed by appropriate organizational personnel.

4. Dynamic and Role-Based Access: Organizations may define access privileges and other attributes either by individual accounts, by account types, or both. This includes factors like time-of-day restrictions, day-of-week restrictions, and point-of-origin restrictions, which can impact account access and system availability.

5. Emergency and Temporary Accounts: These accounts are meant for short-term use. Emergency accounts may bypass normal authorization processes due to the urgency of crisis situations. Temporary accounts are established through standard procedures but are intended for short-term use.

6. Infrequently Used Accounts: Unlike temporary or emergency accounts, infrequently used accounts remain available for specific tasks and are not subject to automatic deactivation.

7. Account Disabling Conditions: Conditions under which accounts are disabled or deactivated include when shared/group, emergency, or temporary accounts are no longer needed, or when individuals are transferred or terminated.

8. Specialized Training: Certain account types, especially those requiring administrative privileges, may need users to undergo specialized training to manage these accounts properly.

Overall, the Supplemental Guidance section aims to ensure organizations consider all relevant factors and best practices for effective account management. It addresses potential challenges and provides strategies to maintain security and operational efficiency in account management processes.

1. What is the Control Enhancements section all about?

The Control Enhancements section of AC-2: Account Management in NIST Special Publication 800-53, Revision 4, specifies additional measures that organizations can implement to strengthen their account management controls. These enhancements provide more detailed or advanced capabilities beyond the basic requirements of the control. Here's a summary of the control enhancements:

1. AC-2(1): Automated System Account Management

- Baseline(s): Moderate, High

- Organizations use automated mechanisms to manage information system accounts, improving efficiency and accuracy in account creation, modification, and deletion.

2. AC-2(2): Removal Of Temporary / Emergency Accounts

-Baseline(s): Moderate, High

- The system automatically removes or disables temporary and emergency accounts after a predefined period, ensuring these accounts do not remain active longer than necessary.

3. AC-2(3): Disable Inactive Accounts

- Baseline(s): Moderate, High

- The system automatically disables accounts that have been inactive for a defined period, reducing the risk of unauthorized access through dormant accounts.

4. AC-2(4): Automated Audit Actions

- Baseline(s): Moderate, High

- The system automatically audits account-related actions (creation, modification, enabling, disabling, removal) and notifies designated personnel, enhancing accountability and traceability.

5. AC-2(5): Inactivity Logout

- Baseline(s): High

- Users are required to log out after a specified period of inactivity, reducing the risk of unauthorized access if users leave their sessions unattended.

6. AC-2(6): Dynamic Privilege Management

- Baseline(s): Not part of any baseline

- The system supports dynamic privilege management capabilities, allowing for real-time adjustments to user privileges based on current conditions or requirements.

7.AC-2(7): Role-Based Schemes

-Baseline(s): Not part of any baseline

- Organizations use a role-based access scheme to manage privileged user accounts, ensuring that access and privileges are organized into roles and monitored appropriately.

8. AC-2(8): Dynamic Account Creation

- Baseline(s): Not part of any baseline

- The system can dynamically create accounts as needed, streamlining the process and ensuring that accounts are created quickly and efficiently.

9. AC-2(9): Restrictions On Use Of Shared / Group Accounts

- Baseline(s): Not part of any baseline

- The organization sets conditions for using shared/group accounts, ensuring they are only used when absolutely necessary and under controlled circumstances.

10. AC-2(10): Shared / Group Account Credential Termination

- Baseline(s): Not part of any baseline

- The system terminates shared/group account credentials when members leave the group, preventing unauthorized access by former group members.

11. AC-2(11): Usage Conditions

- Baseline(s): High

- The system enforces defined usage conditions for accounts, such as time-of-day restrictions or specific usage scenarios, enhancing security controls around account access.

12. AC-2(12): Account Monitoring / Atypical Usage

- Baseline(s): High

- Organizations monitor accounts for atypical usage patterns and report any unusual activity to designated personnel, helping to detect and respond to potential security incidents.

13. AC-2(13): Disable Accounts For High-Risk Individuals

- Baseline(s): High

- Accounts for individuals identified as high-risk are disabled within a defined period after the risk is discovered, mitigating potential threats from these individuals.

Purpose of Control Enhancements

Control enhancements build on the basic requirements of AC-2 by introducing more rigorous, specific, or automated measures to improve the security and management of information system accounts. They help organizations tailor their account management practices to better align with their risk profiles and operational needs.

When you are finished upload this document into Canvas for your submission.