Young Consulting Group | Secure Stack Monthly
www.youngconsultinggrouop.co
admin@youngconsultinggroup.co

Secure Stack Monthly

Issue #1 – Access Control Foundations

Welcome to the first issue of Secure Stack Monthly. Each month we'll break down 2–3 NIST 800-53 controls into plain language, show you how to implement them, and give you usable checklist or template you can apply right away. This month we're focusing on Access Control — specifically, AC-2 (Account Management), AC-3 (Access Enforcement), and AC-6 (Least Privilege). These three controls form the backbone of preventing unauthorized access and ensuring compliance in both classified and unclassified environments.

AC-2: Account Management

Organizations must establish processes to create, manage, review, disable, and remove user accounts in line with policy. Every account should be tied to an authorized user with a documented need.

Implementation checklist:

- Document account request/approval process
- Require managerial approval for new accounts
- Disable inactive accounts after X days (per org policy)
- Review accounts quarterly
- Terminate accounts immediately when users separate

Audit artifacts:

- Account management SOP
- Logs from lastlog or AD reports showing inactive accounts disabled
- Quarterly account review tracker

Common pitfall: Dormant accounts left active — auditors' flag this as a CAT-1.

AC-3: Access Enforcement

Systems must enforce access decisions based on policies (who can do what). This is the technical enforcement of rules defined in AC-2.

Implementation checklist:

- Enforce RBAC (role-based access control) on Linux/Windows systems
- Ensure file system permissions (chmod, chown) align with roles
- Limit sudo privileges to authorized administrators
- Integrate system auth with enterprise directory (LDAP/AD)

Audit artifacts:

- Role definitions document
- System configs (/etc/sudoers, AD group policies)
- Access logs showing enforcement

Common pitfall: Giving users direct root access instead of enforcing RBAC.

AC-6: Least Privilege
Users and processes should only have the minimum access required to perform their duties.

Implementation checklist:
- Assign permissions based on role, not individual
- Remove local admin rights for regular users
- Require privilege elevation (sudo) with justification
- Audit sudo logs regularly (/var/log/secure)

Audit artifacts:
- User-to-role mapping
- Sudo policy or equivalent
- Logs showing periodic review of privileged commands

Common pitfall: All engineers in the admin group — auditors will reject blanket privilege assignments.

Case Study: Privileged Account Oversight
A defense contractor's SIPRNet system was flagged during inspection: 10 users retained sudo privileges after transferring to other projects.
Problem: Violated AC-2 (inactive accounts not removed) and AC-6 (excess privileges).
Impact: Elevated finding, delay in ATO renewal.
Fix: Immediate removal of stale accounts, implementation of quarterly review checklist.
Lesson: Privileged accounts are always scrutinized first by auditors.

Closing & Next Issue
Key takeaways:
1. Every account must have a business owner and justification (AC-2).
2. Systems must technically enforce access rules (AC-3).
3. Excess privilege is the #1 audit finding (AC-6).

Next Issue Preview: We'll dig into Audit & Accountability (AU-2, AU-6, AU-8) — how to prove your logging meets compliance standards.