1 Case Study

When I started as an auditor, I had been an IT Security consultant for a number of years. I thought my first audit report was good enough to alert management to the problem. The Chief Audit Executive (CAE) rejected my report. The CAE strongly recommended that I take a course like this one. After taking that course, the CAE invited me to re-write my report. You can see the differences below. *These are not the actual reports that I submitted, because those are proprietary documents that belong to the company where I worked.*

Looking at these reports side by side, you can see the profound difference: one is trying to fix the system, the other is trying to change management's behavior. For clarity, Report 1 is on the left side in gray text, and Report 2 is on the right side in black text.

Report 1: IT Security Consultant (Action-Oriented, Remediation-Focused)

Subject: Immediate Remediation Plan – Identity and Access Management Weaknesses

A review of Active Directory (AD) indicates material control gaps in identity and access management that present an elevated risk of unauthorized access and potential compromise.

The organization has 1,234 users but maintains 1,754 AD accounts, indicating a significant number of duplicate or unnecessary accounts. A sample review of 200 accounts identified that 27% (54 accounts) lacked documented management authorization, and 30.5% (61 accounts) retained their initial password. Additionally, there is limited assurance that user access aligns with role-based requirements. The use of a consistently renamed local administrator account ("geddy") further reduces security through predictability.

From a security operations perspective, the environment should be treated as potentially overexposed.

Report 2: Audit Report (Structured, Persuasive, Management-Focused)

Subject: Audit of Identity and Access Management Controls

Objective and Scope: To assess whether user account management controls ensure that access is appropriately authorized, provisioned, and maintained in alignment with organizational policies.

Finding 1: Inadequate User Account Authorization and Control

Criteria

- User accounts should be created only with documented management authorization.
- Access should be unique per user and aligned with job responsibilities.
- Initial passwords must be changed upon first use.
- Periodic reviews should validate user access and account validity.

Condition

- The organization maintains 1,754 AD accounts for 1,234 users, indicating duplicate or unnecessary accounts.

Report 1 continued…

Immediate Actions (Next 24–72 Hours)

1. Disable Duplicate Accounts
    a. Identify users with multiple accounts and disable all but one.
    b. Re-enable accounts only after user verification through the help desk.
    c. This will quickly reduce the attack surface.
    d. Force Password Reset
    e. Require password changes for all users at next login.
    f. Immediately reset accounts identified with unchanged initial passwords.
2. Secure Administrator Accounts
    g. Randomize and standardize naming conventions for local admin accounts.
    h. Implement unique credentials and, if possible, privileged access management (PAM).
3. Access Review (Targeted)
    i. Focus first on high-risk groups (administrators, finance, HR).
    j. Remove clearly excessive privileges.

Report 2 continued…

- In a sample of 200 accounts:
    a. 54 (27%) lacked evidence of management authorization.
    b. 61 (30.5%) retained their initial password.
- There is limited assurance that access permissions align with user roles.
- A predictable naming convention is used for local administrator accounts.

Cause

- Lack of enforced provisioning controls requiring documented approval.
- Absence of automated or centralized identity governance processes.
- Insufficient monitoring and periodic review of user accounts.
- Weak enforcement of password and administrative account standards.

Consequence (Impact)

- Increased risk of unauthorized access and privilege misuse.
- Elevated likelihood of account compromise due to unchanged passwords.
- Potential for privilege escalation through duplicate or unmanaged accounts.
- Reduced ability to demonstrate compliance with security and regulatory requirements.
- Predictable administrator account naming increases susceptibility to targeted attacks.

Report 1 continued...

Short-Term Stabilization (Next 30 Days)

- Implement enforced manager approval workflow for all new accounts.
- Introduce automated provisioning controls (no account without approval).
- Establish a centralized identity inventory (single source of truth).

Begin quarterly access certification, starting with critical systems.

Report 2 continued...

Correction (Recommendation)

Management should implement a strengthened identity and access management control framework, including:

1. Account Provisioning Controls
    - Enforce mandatory, documented management approval for all new accounts.
    - Implement automated workflows to prevent account creation without approval.
2. Account Rationalization
    - Identify and remove or disable duplicate and unnecessary accounts.
    - Establish a single unique account per user unless formally justified.
3. Password and Authentication Controls
4. Enforce mandatory password change at first login.
5. Periodically validate compliance with password policies.
6. Privileged Access Controls
    - Eliminate predictable administrator account naming conventions.
    - Implement stronger controls for administrative accounts (e.g., separate credentials, monitoring).
7. Periodic Access Reviews
    - Require quarterly access certification by managers.
    - Ensure timely removal of inappropriate or excessive access.

Report 1 continued...

Observations

The proposed approach by the auditee — to disable duplicate accounts and rely on user calls to restore access — is directionally correct for rapid containment, but should be tightly controlled to avoid operational disruption and social engineering risks.

Summary

The priority is to regain control of identities quickly, reduce exposure, and then stabilize governance. Speed matters here; precision can follow once the environment is under control.

Report 2 continued...

Management Response (Summary)

Management agrees with the findings and has proposed:

- Disabling duplicate accounts and re-enabling access upon user request.
- Implementing improved authorization processes for account creation.
- Initiating quarterly access reviews conducted by managers.

Conclusion / Overall Opinion

The current state of identity and access management controls is not operating effectively. While management has acknowledged the issues and proposed corrective actions, timely and disciplined implementation will be critical to reducing the organization's exposure to unauthorized access and control failures.