

Identity Is the Linchpin: Why Account Audits Matter

A practical control for reducing risk, improving cyber hygiene, and demonstrating responsible oversight.



Most cyber incidents do not begin with an exotic technical failure. They begin with an identity (user account) that is weakly protected, overprivileged, shared, or no longer needed. Because identities are the linchpin to your network, a disciplined user account audit is one of the most practical ways to reduce risk, improve cyber hygiene, and demonstrate responsible oversight.

What an Effective Audit Should Test



Stale accounts

Disable or remove accounts tied to former employees, contractors, abandoned services, or prolonged inactivity.



Users operating with administrator privileges

Separate routine user activity from privileged administration and apply least privilege.



Privilege delegation

Review direct and inherited permissions, role assignments, temporary access, and approval paths.



Unnecessary administrator accounts

Confirm that every privileged account has a current business purpose and an accountable owner.



Inconsistently applied MFA

Identify gaps across users, administrators, remote access, cloud services, and high-risk applications. Every user account should have MFA.



Shared passwords between accounts

Eliminate password reuse and shared credentials; assign unique identities wherever possible.

Poor account hygiene expands the attack surface of your network, weakens accountability, and allows a single compromised credential to cause outsized damage. It also makes investigations slower and can undermine evidence that security controls are operating as intended. Account audits turn identity governance from an assumption into a documented management practice.



Next Steps

Ensure your next audit is scheduled today. Direct internal audit or IT to review user and privileged accounts on a regular schedule—**no less than annually**, and more frequently for high-risk or rapidly changing environments. Require a written record of the scope, findings, accountable owners, remediation actions, exceptions, and completion dates. Executives should receive a concise summary of material risks and verify that unresolved items are tracked to closure.