Access Control Audit – IT & GRC Focus (Mock)

Prepared by: James Gladden
Objective: To evaluate logical access controls, authentication mechanisms, and privilege management to assess alignment with SOC 2 and ISO/IEC 27001 requirements.

Scope

This audit reviews user access provisioning, authentication controls, privileged access management, and access review processes for a small IT environment. The assessment focuses on control design rather than operating effectiveness.

Methodology

The audit was conducted through documentation review, system configuration observation, and control evaluation against SOC 2 Security and ISO/IEC 27001 Annex A access control requirements.

Control Areas Reviewed

User Access Provisioning

Control Objective: User accounts are created based on role and business need.
Observed State: Access provisioning is performed manually with limited documentation.
Recommendation: Establish documented access request and approval procedures.

Authentication & MFA

Control Objective: Multi-factor authentication is used to strengthen access security.
Observed State: MFA enabled for administrative access only.
Recommendation: Expand MFA to all privileged and remote access users.

Privileged Access Management

Control Objective: Privileged accounts are restricted and monitored.
Observed State: Privileged access exists without periodic review.
Recommendation: Implement scheduled privileged access reviews and logging.

Access Reviews

Control Objective: Periodic reviews validate appropriate access.
Observed State: Access reviews conducted informally.
Recommendation: Formalize quarterly access review process and retain evidence.

Account Deprovisioning

Control Objective: User access is removed upon role change or termination.
Observed State: Deprovisioning handled manually.
Recommendation: Document deprovisioning procedures and timelines.

Overall Assessment

The environment demonstrates foundational access control practices; however, formal documentation, periodic reviews, and expanded MFA enforcement are required to strengthen compliance and audit readiness.

Conclusion

Addressing the identified gaps will reduce the risk of unauthorized access and support stronger alignment with SOC 2 and ISO/IEC 27001 access control expectations.