

GRC & IT Audit Portfolio Summary

Prepared by: James Gladden

This document provides an executive summary of Governance, Risk, and Compliance (GRC) and IT audit work completed to demonstrate entry-level audit readiness, control evaluation skills, and familiarity with industry-standard compliance frameworks.

Frameworks Covered

- SOC 2 (Security Trust Services Criteria)
- ISO/IEC 27001 (Annex A Controls)
- General IT Access Control Principles

Audit Methodology Overview

All audits and assessments followed a structured methodology consistent with IT audit and compliance consulting practices. The focus was on evaluating control design rather than operating effectiveness.

Methodology Steps

1. Scope definition and control selection
2. Control objective identification
3. Design evaluation against framework criteria
4. Gap identification and risk articulation
5. Recommendation development and documentation

Completed Audit Engagements

SOC 2 Type I Readiness Assessment

Assessed the design of security controls for a SaaS-style environment against SOC 2 Security criteria. Identified documentation gaps, access control weaknesses, and incident response improvement areas.

SOC 2 Control Assessment Workpapers

Performed control-by-control design assessments including logical access, authentication, change management, incident response, and risk assessment controls. Documented findings and recommendations in audit-style workpapers.

ISO/IEC 27001 Annex A Control Review

Reviewed selected Annex A controls to evaluate implementation status, ownership, and documentation maturity. Identified gaps preventing alignment with ISO/IEC 27001 expectations.

Access Control Audit (IT & GRC)

Evaluated access provisioning, authentication mechanisms, privileged access management, and access review processes. Developed recommendations to reduce unauthorized access risk and improve audit readiness.

Professional Value & Readiness

This portfolio demonstrates the ability to think and operate as an entry-level IT auditor or GRC analyst. Skills demonstrated include control analysis, structured documentation, risk articulation, and alignment with multiple compliance frameworks.

Key Competencies Demonstrated

- Internal control analysis
- Audit documentation and workpapers
- Risk identification and mitigation recommendations
- Framework-based compliance thinking
- Professional communication and reporting

This work is representative of responsibilities typically performed by Staff Consultants, Associate IT Auditors, and entry-level GRC analysts during client engagements.