SOC 2 Type I Readiness Assessment (Mock)

Prepared by: James Gladden

Audit Overview

This mock SOC 2 Type I Readiness Assessment evaluates the design of security controls for a small SaaS-style environment. The objective is to assess whether controls are suitably designed to meet the SOC 2 Security Trust Services Criteria and to identify gaps prior to a formal audit.

Scope

The assessment focuses on the Security Trust Services Criteria, including access controls, system monitoring, logical security, and risk management processes. Operating effectiveness testing was not performed.

Methodology

The readiness assessment was conducted through documentation review, control identification, risk analysis, and comparison against SOC 2 Security criteria. Findings were documented in audit-style workpapers.

Control Assessment Summary

Key controls reviewed included user access management, authentication mechanisms, incident response awareness, and system configuration practices. Controls were assessed for design adequacy and alignment with SOC 2 expectations.

Findings & Risks

Identified risks included inconsistent access reviews, limited formalized incident response documentation, and lack of periodic control validation. These gaps may increase the risk of unauthorized access or delayed response.

Recommendations

Recommendations include formalizing access review procedures, documenting incident response workflows, and implementing periodic control assessments to support audit readiness.