# SOC 2 Type I – Control Assessment Workpapers (Mock)

Prepared by: James Gladden
Purpose: To assess the design of key security controls against SOC 2 Trust Services Criteria.

**CC6.1 – Logical Access Controls**

**Control Description:** The organization restricts logical access to systems and data to authorized users only.
**Observed Design:** Access is managed through unique user accounts and role-based permissions.
**Design Assessment:** Design Adequate
**Identified Gap:** Access reviews are informal and not documented.
**Recommendation:** Formalize quarterly access reviews and retain evidence.

**CC6.2 – Authentication Mechanisms**

**Control Description:** The organization uses authentication mechanisms to prevent unauthorized access.
**Observed Design:** Multi-factor authentication is enabled for administrative access.
**Design Assessment:** Design Adequate
**Identified Gap:** MFA is not enforced for all user roles.
**Recommendation:** Expand MFA enforcement to all privileged and remote access users.

**CC7.2 – Security Incident Response**

**Control Description:** The organization responds to detected security incidents in a timely manner.
**Observed Design:** Incident response steps are understood but not formally documented.
**Design Assessment:** Partially Adequate
**Identified Gap:** Lack of documented incident response plan.
**Recommendation:** Create and maintain a formal incident response policy and procedures.

**CC8.1 – Change Management**

**Control Description:** The organization authorizes, tests, and approves system changes.
**Observed Design:** System changes are performed but lack formal change records.
**Design Assessment:** Partially Adequate
**Identified Gap:** Changes are not consistently documented.
**Recommendation:** Implement change logs and approval documentation.

**CC9.2 – Risk Assessment**

**Control Description:** The organization identifies and assesses risks related to system security.
**Observed Design:** Risk identification is performed informally.
**Design Assessment:** Partially Adequate
**Identified Gap:** No formal risk assessment schedule.
**Recommendation:** Establish periodic documented risk assessments.