SOC 2 REPORT

Capstone Project

By Tanasha Bryant

**Introduction**

**Purpose of the Report**

This report provides an overview an approach to achieving SOC 2 compliance. It outlines the benefits of obtaining a SOC 2 audit, the recommended audit type, prioritize Trust Services Criteria, implemented security controls, and the corresponding test descriptions to evaluate control effectiveness.

**Company Overview**

Logger is a US-based company offering a 24x7x7365 SOC-as-a-Service platform that enables organizations to collect and analyze terabytes of log data. The platform is hosted on Microsoft Azure and provides machine-learning-based alerting, role-based access controls, and multi-factor authentication. Logger aims to expand into Fortune 500 market, particularly in regulated industries such as Finance and Healthcare, making SOC 2 compliance essential for its business growth.

**Benefits of Obtaining a SOC 2 Audit**

**Logger will benefit from SOC 2 compliance in the following ways:**

* **Competitive Advantage**: Compliance with SOC 2 will differentiate Logger from competitors and improve credibility when selling to larges enterprises.
* **Market Expansion**: Many Fortune 500 companies require vendors to have a SOC 2 report before entering business agreements, especially in regulated industries.
* **Operational Security Improvements**: The SOC 2 readiness and audit process will help Logger refine internal security controls and strengthen data protection measures.
* **Enhanced Customer Trust**: SOC 2 certification will assure customers that Logger follows industry best practices for security and compliance.

**Recommended SOC 2 Audit Type**

Logger should pursue a SOC 2 Type II audit. This provides a high level of assurance to potential customers, demonstrating Loggers ongoing commitment to security and compliance. The audit should take 6 – 12 months to complete.

**Prioritized Trust Services Criteria**

**Based on Logger’s business model and expansion goals, the following three Trust Services Criteria (TSC) are most relevant:**

* **Security (CC Series 6 -7)** – Critical for protecting sensitive log data against unauthorized access and cyber threats.
* **Availability (CC Series 8)** – ensures Logger meets its uptime commitments and provides reliable services to customers.
* **Confidentiality (CC Series 9)** – essential for safeguarding customer data and managing vendor risk effectively.

**Implemented Security Controls**

Logger has established the following security controls to meet SOC 2 compliance requirements:

* **CC.6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users who whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.** 
  + Control: Logger verifies all internal and external users prior to granting system access. Logger reviews user credentials of both internal and external employees upon employee termination.
* **CC.7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify changes to configuration that result in the introduction of new vulnerabilities, and susceptible to newly discovered vulnerabilities.** 
  + Control: Logger conducts automated vulnerability scans to detect configuration changes and security threats. High-risk vulnerabilities must be remediated within 30 days.
* **CC.7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.** 
  + Control: Logger has an incident response plan covering identification, containment, remediation, and communication. Security incidents are documented, and a post-incident review conducted.
* **CC.8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.** 
  + Control: Logger follows a formal process for infrastructure and software changes including documentation, testing, approval, and implementation.
* **CC.9.2 – The entity assesses and manages risks associated with vendors and business partners.** 
  + Control: Logger conducts annual security assessments for all-third-party vendors handling sensitive data and require compliance agreements.

**Test Descriptions for Control Effectiveness**

The following test descriptions outline how each controls effectiveness will be evaluated:

* **CC.6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users who whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.** 
  + Test: Reviewed a sample of user access request for the last 2 quarters to verify they were properly approved and documented. Checked if the employees had their access revoked within 24 hours.
* **CC.7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify changes to configuration that result in the introduction of new vulnerabilities, and susceptible to newly discovered vulnerabilities.** 
  + Test: Observed Logger perform vulnerability scans and reviewed reports from the past 3 months to confirm that high risk vulnerabilities were identified and remediated at the time of detection.
* **CC.7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.** 
  + Test: Inspected Loggers incident response documentation for the past year. Selected at least two incidents and verified that containment, remediation, and post-incident review steps were completed as per policy.
* **CC.8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.** 
  + Test: Requested a sample of change requests from Logger as needed and confirmed that each followed the documented change management process. (including approval, testing, and implementation steps)
* **CC.9.2 – The entity assesses and manages risks associated with vendors and business partners.** 
  + Test: Reviewed a sample of vendor security assessments conducted in the past year to ensure compliance with Logger’s vendor management policy. Checked for documented risk evaluations and security agreements.