SOC 2 COMPLIANCE PROJECT PLAN

SOC stands for System and Organization Controls and represents a set of compliance standards developed by the American Institute of CPAs (AICPA) – a network of over 400,000 professionals across the globe. SOC Audits aim to examine the policies, procedures, and internal controls of an organization.

SOC 2 applies to any organization wanting to effectively demonstrate to associated organizations controls associated with regard to Security, Availability, Confidentiality, Processing Integrity and Privacy or any combination of these as part of third-party relationships. It is also applicable to organizations that store its customer data in the cloud as well as Third-party service providers such as cloud storage, web hosting and software-as-a-service (SaaS) companies.

SOC Compliance & Certification

There are 3 types of
SOC Audits and Reports

□ SOC 1 (Financial Controls)

Reports on the processes and controls that influence the organization's internal control over financial reporting (ICFR). SOC 1 is also a standard assessment report required by user entities to comply with Sarbanes-Oxley Act (SOX).

□ SOC 2 (IT Controls)

Designed for service organizations and reports on non-financial controls. Focuses on five key trust services criteria (formerly called trust services principles), or TSCs. SOC 2 outlines the standards that are necessary to keep sensitive data private and secure while it's in transit or at rest.

□ SOC 3 (Publicly Shareable)

SOC 3 is similar to SOC 2 in terms of the audit criteria. The main difference is in the reporting - SOC 2 is tailored for sharing with specific organizations, whereas SOC 3 reports are more applicable for general audiences and therefore made publicly available.

SOC 2 COMPLIANCE PROJECT PLAN

□ Task 1: ORGANIZATIONAL BUY-IN

☑ Organization wide announcement on the SOC 2 compliance initiative, give clarity on how SOC 2 Compliance will help the business:

-Ensure security controls are in-place against data breaches
-Demonstrate to customers that the organization has addressed controls against service level agreements
-Qualify for more RFPs and attract more clients

□ Task 2: IDENTIFY KEY PERSONNEL AND ROLES

☑ Engage ControlCase for end-to-end delivery of SOC 2 Attestation

☑ Identify key roles within the organization that will assist with evidence collection

- Key roles include, but are not limited to subject matter experts (SMEs) in the following:

  - Legal
  - Information Technology and Information Security
  - Compliance
  - Engineering
  - Software developers
  - Human Resources
  - Executive management
  - Operations
  - Physical security

□ Task 3: SCOPING

☑ ControlCase can assist in the selection of the appropriate Trust service Criteria that are applicable to the business, thereby reducing scope, ensuring accuracy and minimizing cost.

  - Applicable Trust Criteria
  - Identification of Internal Key Controls

□ Task 4: OBSERVATION PERIOD

☑ **SOC 2 Type I** attestation evaluates the controls at a specific point in time. (As of date)

☑ **SOC 2 Type II** attestation evaluates controls over an extended period retrospectively to ensure the effectiveness of the controls (normally no less than 6 months and no more than 12).

□ Task 5: POLICY PROCEDURE & REVIEW

☑ Required Policy Documents (templates available for ControlCase Clients) can include, but is not limited to:

  - Information Security Policy
  - Access Control Policy
    - ▪ Physical Access Procedure
  - Human Resource Policy
  - Network Security Policy
  - Password Management Policy
  - Physical Access Policy
  - Remote Access Policy
  - Risk Assessment Methodology

ABOUT CONTROLCASE:

ControlCase is a global provider of certification, cyber security and continuous compliance services. ControlCase is committed to empowering organizations to develop and deploy strategic information security and compliance programs that are simplified, cost effective and comprehensive in both on-premise and cloud environments. Control-Case offers certifications and a broad spectrum of cyber security services that meet the needs of companies required to certify to PCI DSS, HITRUST, SOC 2 Type II, ISO 27001, PCI PIN, PCI P2PE, PCI TSP, PCI SSF, CSA STAR, HIPAA, GDPR, SWIFT and FedRAMP.