SOC 2 COMPLIANCE CHECKLIST

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 CHECKLIST

Examples of what is addressed under the (5) SOC 2 Trust Service Criteria (TSCs):

□ SECURITY

- □ Pen tests & vulnerability assessments
- □ Application security measures
- □ Firewalls
- □ Intrusion detection systems (IDS)
- □ Multi factor authentication tools
- □ Access Control
- □ Application & Network Security Measures
- □ Computer Use Policies

□ AVAILABILITY

- □ Performance & incident monitoring, response
- □ Disaster response and recovery
- □ Secure data backups

□ PROCESSING INTEGRITY

- □ Quality Assurance
- □ Process Monitoring Sysstems

□ CONFIDENTIALITY

- □ Digital access controls
- □ Physical access controls
- □ Network & application firewalls
- □ Crypotgraphic solutions

□ PRIVACY

- □ Notice and communication of objectives
- □ Choice and consent
- □ Collection
- □ Use, retention, and disposal
- □ Access
- □ Disclosure and Notification
- □ Quality
- □ Monitoring and enforcement

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. ControlCase 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.

For more information email contact@controlcase.com