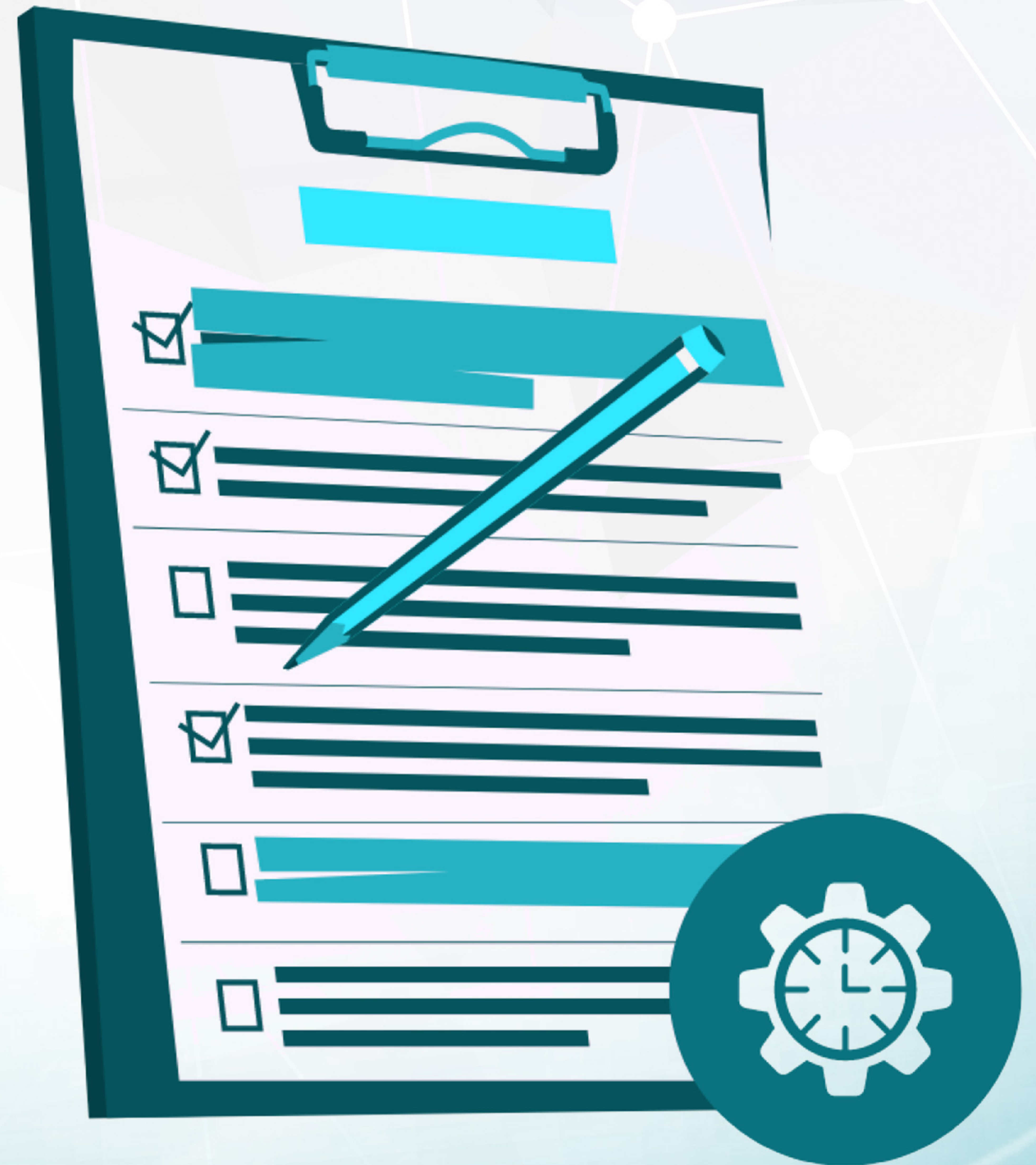


SOC 2

Compliance Checklist



1. Define Scope and Objectives

- ☐ Identified the systems/services that processed or stored client data
- ☐ Determined which Trust Services Criteria applied:
 - Type I – Security (mandatory)
 - Type II – ☒ Availability, Processing Integrity, Confidentiality, Privacy (optional based on service commitments)
- ☐ Selected a CPA firm with demonstrated experience in IT systems and cybersecurity audits
- ☐ Reviewed third-party relationships to define relevant Complementary Subservice Organization Controls (CSOCs)
- ☐ Outlined necessary Complementary User Entity Controls (CUECs) based on system dependencies



Tip: Consult the auditor at this stage to ensure your scope aligns with customer expectations and market needs.

2. Security (Common Criteria – Required)

Organizational Controls

- ☐ Documented information security policy, approved and reviewed annually
- ☐ Clear assignment of information security roles and responsibilities

Access Controls

- ☐ Enforcement of strong passwords and MFA
- ☐ Role-based access control (RBAC) and least privilege principle
- ☐ Timely user provisioning and de-provisionin
- ☐ Periodic access reviews

System Operations & Monitoring

- ☐ Centralized logging and SIEM monitoring in place
- ☐ Regular vulnerability scans and risk assessments
- ☐ Tested and documented incident response plan
- ☐ Endpoint protection and anti-malware controls

Change Management

- ☐ Formalized change approval workflows
- ☐ Segregated development and production environments
- ☐ Pre-deployment change testing and documentation

Risk Management

- ☐ Annual risk assessments conducted and documented
- ☐ Active risk treatment plans in place

3. Availability (If in Scope)

- ☐ SLAs and uptime targets defined and monitored
- ☐ System capacity regularly evaluated
- ☐ Annual testing of backup and disaster recovery plans
- ☐ Documented escalation procedures for incidents

4. Processing Integrity (If in Scope)

- ☐ Input/output data validation processes in place
- ☐ Logging and review of processing activities
- ☐ Timely error detection and correction controls
- ☐ Confirmation of completeness and accuracy of transactions

5. Confidentiality (If in Scope)

- ☐ Data classification policy enforced
- ☐ Encryption of confidential data (in transit and at rest)
- ☐ NDAs signed by vendors and staff handling sensitive data
- ☐ Secure media disposal procedures

6. Privacy (If in Scope)

- ☐ Published privacy notice aligned with current practices
- ☐ Consent processes for data collection and processing
- ☐ Mechanisms to support data subject rights (access, correction, deletion)
- ☐ Documented personal data retention schedule

7. Vendor Management

- ☐ Vendor risk assessments completed
- ☐ SOC 2 or equivalent assurance reports collected from critical third parties
- ☐ Contracts include data protection and security clauses
- ☐ Ongoing vendor evaluations and reviews conducted

8. Audit Readiness & Documentation

- ☐ Policies and procedures are documented, version-controlled, and accessible
- ☐ Evidence logs and artifacts collected and organized
- ☐ Control owners identified and trained
- ☐ Gap analysis or readiness assessment completed prior to formal audit

9. Ongoing Compliance

- ☐ Quarterly self-assessments of controls
- ☐ Annual internal or third-party reviews
- ☐ Annual training on security and privacy practices for all employees'
- ☐ Continuous policy updates as technologies and laws evolve

 **Tip:** A qualified auditor will help validate your readiness and interpret Trust Services Criteria specific to your environment.

Have any questions regarding SOC 2 compliance?

Schedule a free consultation with our experienced compliance strategists now!

Contact Us

Visit Us: <https://vistainfosec.com/>



<https://www.linkedin.com/company/vistainfosec/>



www.youtube.com/@Vistainfosecofficial



twitter.com/vistainfosec



facebook.com/vistainfosec

Contact Us: [sales\(at\)vistainfosec.com](mailto:sales(at)vistainfosec.com)

USA: +1-415-513-5261 Singapore: +65-3129-0397

India: +91 998724469 UK: +442081333131