SOC 2

Overview & Purpose

- Developed by AICPA
- For Service Organizations
- Based on Trust Services Criteria (TSC)
- Audited by licensed CPA firms
- Voluntary but widely required by clients

Report Types

- SOC 2 Type I
  - Point-in-time assessment
  - Design of controls only
- SOC 2 Type II
  - Period of time (min. 6 months)
  - Design & operating effectiveness
- SOC 2+
  - SOC 2 + additional framework mapping
  - e.g. HIPAA, HITRUST, ISO 27001

5 Trust Services Criteria (TSC)

- Confidentiality (Optional)
  - Designated confidential info protected
  - Encryption, access controls
- Privacy (Optional)
  - Personal info collected, used & disclosed per privacy notice
  - Aligned with AICPA Privacy Management Framework
- Security (CC – Required)
  - Common Criteria (CC1–CC9)
  - Protection against unauthorized access
  - Mandatory for all SOC 2 audits
- Availability (Optional)
  - System accessible as agreed
  - Uptime, performance monitoring
- Processing Integrity (Optional)
  - Complete, valid, accurate processing
  - Timely & authorized transactions

Common Criteria Categories (CC)

- CC1 – Control Environment
- CC2 – Communication & Information
- CC3 – Risk Assessment
- CC4 – Monitoring Activities
- CC5 – Control Activities
- CC6 – Logical & Physical Access
- CC7 – System Operations
- CC8 – Change Management
- CC9 – Risk Mitigation

Key Stakeholders

- Service Organization (auditee)
- User Entity (client / customer)
- CPA / Audit Firm (service auditor)
- Subservice Organizations (vendors / subprocessors)
- Management & Board (governance)

Audit Process

1. Define Scope & Criteria
2. Readiness Assessment (Gap Analysis)
3. Remediate Control Gaps
4. Auditor Fieldwork & Evidence Collection
5. Management Assertion
6. Auditor Issues Opinion & Report
7. Annual Renewal Cycle

Key Controls & Evidence

- Access Management (MFA, RBAC, reviews)
- Encryption (in-transit & at-rest)
- Vulnerability Management & Pen Testing
- Incident Response Plan & Testing
- Change Management & SDLC
- Business Continuity & Disaster Recovery
- Vendor / Third-Party Risk Management
- Security Awareness Training
- Logging & Monitoring (SIEM)
- Background Checks & HR Policies

Report Sections

- Subservice Organization Controls
- Complementary User Entity Controls (CUECs)
- Trust Services Criteria & Controls (Section IV)
- Independent Auditor's Report
- Management's Assertion
- System Description (Section III)

Auditor Opinion Types

- Disclaimer of Opinion
- Adverse Opinion (material deviation)
- Unqualified (Clean) Opinion
- Qualified Opinion (scope limitation)

SOC 2 vs Other Frameworks

- HITRUST – Healthcare Focused
- FedRAMP – US Federal Cloud
- CSA STAR – Cloud Security
- SOC 1 – Financial Reporting Controls
- SOC 3 – Public Seal Report
- ISO 27001 – ISMS Certification

Continuous Compliance

- Continuous Control Monitoring (CCM)
- Automated Evidence Collection
- GRC / Compliance Platforms (Vanta, Drata, Secureframe)
- Annual Re-audit Requirement
- Risk Register Maintenance

www.hackingarticles.in

@hackinarticles

https://github.com/Ignitetechnologies

https://in.linkedin.com/company/hackingarticles