VIVID OPS

Scoping - SOC 2 Engagements

This questionnaire outlines the information needed to define the scope of your attestation engagement. It supports both readiness reviews and independent audits. Use it to prepare internally, or as a guide for your kickoff with our team.

Engagement Overview

- What type of report is requested? (SOC 1, SOC 2, or SOC 3)
- Will this be a Type 1 or Type 2 report?
- For Type 2, what is the reporting period or coverage timeframe?
- Which of the following Trust Services Criteria apply?
  - Security (required)
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- What is your target delivery deadline?

System and Business Profile

- Provide a brief description of the system, service, or process being evaluated.
- What services, products, or infrastructure components are included in the audit scope?
- What cloud platforms or technology stacks are in use (e.g., AWS, Azure, GCP, etc.)?
- How many employees (or contractors) have access to in-scope systems?
- What is the geographic footprint of your business? Are there international operations?
- Do you collect or process personal data from EU residents?
- Do you collect or process personal data from residents of any US states with privacy laws (e.g., California, Colorado, Virginia)?
- Does your company collect, store, or transmit any of the following types of information, or work with vendors that do?

  - Full names, addresses, dates of birth, Social Security numbers
  - Credit card or payment card data
  - Personal income or credit history
  - Medical records or healthcare-related data
  - None of the above

- Does your company operate in any of the following sectors or provide any of the following services?
  - Payroll processing
  - Debt collection
  - Financing, loans, or mortgages
  - Real estate settlement services
  - Investment advisory or financial consulting
  - Legal services
  - Data processing
  - Third-party administration
  - Insurance
  - None of the above

- Does your company provide consumer credit reports, report data to credit agencies, or issue consumer credit?

Industry, Structure, and Special Conditions

- In what industry or sector does your organization primarily operate?
- Does your organization accept, transmit, or store credit card data?
- Is your company publicly traded, preparing to go public, or serving clients who are publicly traded?
- Does your organization receive federal research grants or other federal funding?
- Does your company handle Controlled Unclassified Information (CUI)?
- Does your organization work with the US federal government, Department of Defense, or contractors supporting federal entities?
- Do you use artificial intelligence (AI) or machine learning technologies in your products, services, or internal operations?

Controls, Readiness, and Documentation

- Approximately how many internal controls are in scope?
- Please estimate and categorize as manual, automated, or hybrid.
- Have you completed a readiness assessment? If yes, when?
- Have you completed a SOC 2 (or SOC 1/3) audit in the past? If so, can we review the latest report?
- Are policies, procedures, and system documentation readily available for review?
- Have you engaged any other CPA firm for this system or reporting period?
- Are you currently using any compliance automation platforms (e.g., Drata, Vanta, Secureframe)?
- How quickly can your team respond to requests for evidence or supporting documentation?

VIVID OPS

Trust Services Criteria (TSC) – Detailed Areas

Security

Organizational Security Management

- How is your information security program structured? Describe roles, reporting lines, leadership oversight, and how policies apply across office-based, hybrid, and remote work environments.

Access Control and Authentication

- What access controls are in place for critical systems and data? Include details on role-based access, password policies, and multi-factor authentication.

Network and Endpoint Protections

- Which security technologies or practices are in place?
    - Firewalls or perimeter protection tools
    - Data encryption (at rest and in transit)
    - Anti-malware software on all endpoints
    - Intrusion detection and prevention systems
    - Network and application activity logging
    - Secure configuration baselines for systems
    - Regular vulnerability scans or penetration tests
    - None of the above

Incident Response Management

- Do you have a formal incident response plan? Is it tested periodically through simulations or drills? How are vulnerabilities remediated?

Employee Awareness and Training

- How often do you provide security training to employees and contractors? Does it cover confidentiality, data handling, and remote work expectations?

VIVID OPS

Availability

System Uptime and Performance Monitoring

- How do you monitor system availability and performance? Include tools used, metric tracking, and capacity planning strategies.

Disaster Recovery and Business Continuity

- Do you maintain documented plans for disaster recovery and continuity of operations? How frequently are they tested or updated?

Processing Integrity

Data Processing and Validation Controls

- What controls ensure that data processing is complete, accurate, timely, and authorized? Include automated validations, reconciliations, and error detection.

Confidentiality

Confidential Data Protection Measures

- How is confidential data classified and protected across the organization? Include encryption, access restrictions, and secure handling policies.

Privacy

Privacy Policy and Governance

- Do you maintain documented privacy policies governing the collection, use, sharing, and disposal of personal information?

Consent and Data Subject Rights

- How does your organization handle requests to access, correct, or delete personal data? Do you have defined processes for managing consent and data subject rights?

VIVID OPS

Other - Vendor and Risk Management

Vendor Risk Management

- How do you assess and monitor the security posture of third-party vendors and service providers? Include onboarding evaluations, annual reviews, and contract requirements.

Asset Inventory and Tracking

- How does your company track physical devices, software, and sensitive data assets? Do you use automated tools or manual processes? Is your inventory current?

Enterprise Risk Management

- Is there a documented process for identifying and mitigating risks across the five Trust Services Criteria?
- How often is it reviewed or updated?