Apptega

GUIDE

SOC 2

Compliance Guide

Understanding and Implementing the
AICPA Trust Services Criteria (TSC)

Current as of November 3, 2025

1. Introduction

SOC 2 is a security and assurance standard used to evaluate the effectiveness of controls over systems relevant to the Trust Services Criteria. A SOC 2 program formalizes security, availability, confidentiality, processing integrity, and privacy controls, and verifies their operation over time. It supports customer trust, contract commitments, and risk-based governance for operational environments.

This section introduces the SOC 2 framework, its objectives, and the program mindset required to operate in a continuously auditable state. SOC 2 requires disciplined execution, documented accountability, and structured control processes supported by evidence.

1A. Beginner Quick-Start (First 30—90 Days)

This structured onboarding roadmap accelerates SOC 2 readiness by focusing on early control adoption, documentation, and evidence discipline. It establishes baseline governance, core security practices, and readiness checkpoints that align with Type I and Type II audit expectations.

Days 1—30: Establish Foundation

- Assign Executive Sponsor and SOC 2 Program Owner
- Define scope and system boundaries
- Draft System Description and architecture diagrams
- Publish core security and IT governance policies
- Establish evidence management structure and naming format
- Initiate risk assessment and identify gaps

Days 31—60: Operationalize Key Controls

- Enforce MFA across in-scope systems
- Implement user provisioning and offboarding workflows
- Configure logging and monitoring baselines
- Establish change management review and approvals
- Validate backups and recovery process
- Begin routine evidence collection

Days 61—90: Validate & Prepare for Audit

- Finalize System Description
- Conduct internal control walkthroughs
- Execute access reviews and log review cycles
- Validate vendor SOC reports, bridge letters, and CUECs
- Document exceptions and track remediation
- Complete readiness gate prior to Type I audit

2. Scope & Applicability

This section defines the systems, services, users, and environments included in the SOC 2 program. Correct scoping ensures that all relevant components that store, transmit, or process customer data and service commitments are covered by controls and evidence.

Scope must be aligned to system boundaries, identity sources, infrastructure layers, data flows, and operational processes. Scope is reviewed at least annually and upon material technology or service changes.

In-Scope Components

- Production systems and supporting services
- Identity and authentication systems
- Personnel with access to in-scope data or environments
- Cloud infrastructure and hosting platforms
- Third-party providers supporting relevant functions

3. Policy Areas & Practices (Trust Services Criteria)

This section defines the control domains required under the AICPA Trust Services Criteria. These criteria provide the foundation for SOC 2 compliance and represent the core operational and security requirements evaluated during the examination period. Each domain includes the objective, key control requirements, and expected evidence demonstrating control effectiveness.

3.1 Security (Common Criteria — CC)

Security establishes baseline requirements for protecting systems and data against unauthorized access, unauthorized disclosure, system misuse, and related threats. These criteria apply to every SOC 2 engagement and form the core control set for the program.

Key Practices

- Formal security governance and control ownership
- Access control and identity management
- Change management and configuration oversight
- System monitoring, logging, audit trails
- Incident response readiness and reporting
- Risk assessment and mitigation practices
- Vendor and subservice provider oversight

Evidence Examples

- Access review logs
- Change tickets with approvals
- Audit logs from production systems
- Incident response records
- Risk register entries and reviews
- Vendor SOC reports and bridge letters

3.2 Availability

Availability ensures that systems operate consistently and reliably to meet service delivery expectations. These controls support system uptime, performance, resilience, and continuity.

Key Practices

- Capacity management and performance monitoring
- Redundancy, failover, and recovery capability
- Data backup protection and restore testing
- Incident and outage procedures
- Business continuity and disaster recovery planning

Evidence Examples

- System uptime reports
- Performance monitoring dashboards
- Backup logs and restoration tests
- DR exercise documentation
- Capacity and scaling reports

3.3 Processing Integrity

Processing Integrity ensures that systems process data accurately, completely, and in a timely manner. These controls support reliable execution of transactions and automated workflows.

Key Practices

- Input, processing, and output validation
- Error handling, reconciliation, and exception logs
- Data quality controls
- Authorization and workflow validation
- Change control over processing logic

Evidence Examples

- Application audit logs
- Error and exception reports
- Reconciliation logs
- QA and testing records for system changes

3.4 Confidentiality

Confidentiality protects sensitive data from unauthorized access and disclosure. These controls focus on safeguarding data classified as confidential throughout its lifecycle.

Key Practices

- Data classification and handling requirements
- Encryption in transit and at rest
- Secure data disposal and retention controls
- Restricted access to confidential information
- Monitoring for unauthorized access attempts

Evidence Examples

- Encryption configuration screenshots
- Data classification documentation
- Data disposal logs
- DLP or access monitoring reports

3.5 Privacy (if included in audit scope)

Privacy controls support the proper collection, use, retention, disposal, and disclosure of personal information in accordance with policies and commitments. This category aligns with privacy requirements applicable to customer personal data.

Key Practices

- Defined notice and consent practices
- Personal data access and correction procedures
- Secure handling and retention of personal data
- Data minimization and purpose limitation
- Privacy complaint handling procedures

Evidence Examples

- Privacy notices and consent logs
- Subject request logs
- Retention documentation
- Privacy incident response evidence

4. RACI Matrix & Accountability Model

Clear accountability ensures SOC 2 controls are consistently designed, implemented, monitored, and evidenced. This section defines responsibility for governance, execution, oversight, and validation functions across the SOC 2 program. Roles and functional groups are mapped to core SOC 2 responsibilities to support transparency, traceability, and audit-ready ownership. Effective SOC 2 operations require distributed accountability supported by executive sponsorship, centralized compliance ownership, and clearly defined technical and business roles.

RACI Legend

- **R** = Responsible (executes the task)
- **B** = Accountable (final authority and ownership)
- **C** = Consulted (provides input)
- **I** = Informed (kept aware)

SOC 2 Accountability Matrix

Function / Activity	Role Title	Function/Department	R	A	C	I
SOC 2 Program Leadership	SOC 2 Program Owner	Compliance	R	A	C	I
Security Governance	CISO	Security	R	A	C	I
Executive Oversight	Executive Sponsor	Executive Leadership		A	C	I
System Description Ownership	CTO	Technology Leadership	R	A	C	I
Risk Management & Assessment	Risk Manager	Risk / Compliance	R	A	C	I
Identity & Access Management	IAM Lead	IT / Security	R	A	C	I
Change Management	Engineering Manager	Engineering	R	A	C	I
Infrastructure & Cloud Security	DevOps Lead	Engineering / DevOps	R	A	C	I
Application Security & SDLC	AppSec Lead	Security Engineering	R	A	C	I
Logging & Monitoring	Security Operations Lead	SecOps	R	A	C	I
Incident Response	IR Manager	Security	R	A	C	I
Disaster Recovery & Continuity	Infrastructure Lead	IT / Engineering	R	A	C	I
Vendor & Subservice Oversight	Vendor Risk Manager	Security / Procurement	R	A	C	I
Training & Awareness	HR + Security Training Lead	HR / Security	R	A	C	I
Evidence Management & Audit Support	Compliance Analyst	Compliance	R	A	C	I
Internal QA & Readiness Testing	Internal Audit Lead	Internal Audit / Quality	R	A	C	I

5. Governance & Program Structure

Effective SOC 2 compliance requires formal governance to ensure leadership accountability, program direction, and continuous adherence to control requirements. Governance establishes oversight, reporting requirements, escalation pathways, and decision-making structure that support sustained audit readiness and operational security maturity.

SOC 2 governance includes executive sponsorship, program ownership, documented roles, review cadences, and control accountability aligned to organizational structure and responsibilities.

Program Governance Structure

- Executive Sponsor responsible for high-level accountability and resource support
- SOC 2 Program Owner responsible for execution, reporting, and audit coordination
- Defined control owners assigned to each control domain and operating responsibility
- Formal committee or recurring working group meetings to review program status
- Documented exception and waiver process for control deviations
- Annual program review and re-authorization by leadership

Program Oversight Cadence

- Executive briefings on SOC 2 status and readiness
- Quarterly control review and validation checkpoints
- Annual risk assessment and policy review cycle
- Continuous evidence collection and internal quality checks

6. System Description Requirements (AICPA DC1-DC14)

The System Description is a foundational component of the SOC 2 report. It defines the boundaries, components, services, and control environment in scope for the examination. It must accurately represent technology, processes, and data handling as they operate in practice. The System Description must be complete, current, and traceable to supporting evidence.

This section outlines required system description elements in accordance with AICPA Description Criteria (DC1–DC14), along with key checkpoints to ensure completeness and audit readiness.

DC1 — Nature of the Services Provided

Defines what the system does, who it serves, and the services delivered.

Checklist

- Description of business purpose and services
- Customer base or service audience
- Key service functions and capabilities
- Delivery model (SaaS, managed service, etc.)

DC2 — Principal Service Commitments & System Requirements

Documents commitments made to users and the requirements needed to fulfill them.

Checklist

- Customer obligations and commitments
- SLAs, security standards, confidentiality promises
- Regulatory or contractual obligations
- Availability and support expectations

DC3 — Components of the System Used to Provide Services

Identifies system components supporting service delivery.

Checklist

- Infrastructure (compute, network, storage)
- Software and platforms
- Data flows and storage points
- People roles and access levels
- Procedures and operational processes
- Supporting vendor/subservices

DC4 — System Boundaries

Defines in-scope and out-of-scope components.

Checklist

- Defined production environment
- Segmented or excluded environments (e.g., dev/test)
- Identity sources and network boundaries
- Shared responsibility models (e.g., cloud services)

DC5 — System Inputs

Describes inputs the system receives.

Checklist

- Data inputs accepted
- Data ingestion sources and mechanisms
- Access points for data entry
- Controls over data input validation

DC6 — System Processes

Explains how the system processes data.

Checklist

- Process flow diagrams
- Transformation logic or transactional workflows
- Automation and validation steps
- Error handling and exception processing

DC7 — System Outputs

Identifies outputs the system generates.

Checklist

- System outputs and reporting features
- Output delivery mechanisms
- Output accuracy controls

DC8 — Data Flow

Documents how data enters, moves through, and exits the system.

Checklist

- Full data lifecycle mapping
- Data storage and retention locations
- Data transfer mechanisms internally and externally

DC9 — System Infrastructure

Defines architectural components.

Checklist

- System architecture diagrams
- Network layout and segmentation
- Cloud hosting and platform services
- Resource isolation mechanisms

DC10 — Logical & Physical Components

Identifies physical and logical architecture.

Checklist

- Hosting and data center information
- Virtualization, containers, serverless
- Physical security considerations (if applicable)

DC11 — Software Components

Outlines software used by the system.

Checklist

- Application stack and dependencies
- Third-party libraries and frameworks
- CI/CD pipeline and build artifacts

DC12 — People & Roles Supporting the System

Defines human involvement in operations.

Checklist

- **Operational roles and responsibilities**
- **Access privileges by role**
- **Separation of duties**

DC13 — Procedures Supporting Service Delivery

Outlines procedures ensuring system operation.

Checklist

- Key operational procedures
- Monitoring and escalation processes
- Incident response procedures
- Maintenance and update cycles

DC14 — Data Retention & Disposal

Explains data retention and destruction practices.

Checklist

- Retention schedules
- Secure disposal controls
- Documentation of disposal events
- Customer data removal processes

System Description Expectations

- Version-controlled and updated at least annually
- Updated when material changes occur
- Traceable to architecture diagrams, access lists, and logs
- Aligned to evidence repository and audit scope

7. Risk Assessment & Treatment Methodology

A formal risk management process ensures that threats and vulnerabilities relevant to systems and services are identified, evaluated, prioritized, and addressed. Risk assessment supports control selection, evidence prioritization, remediation planning, and security investment decisions. SOC 2 requires ongoing risk identification and treatment aligned to business and security objectives.

The risk program must maintain documented risk inputs, assessment criteria, assigned risk ownership, and defined treatment actions with evidence of execution and review.

Key Risk Management Practices

- Maintain formal documented risk assessment
- Define risk criteria and scoring approach
- Identify assets, threats, and vulnerabilities
- Assess likelihood and impact
- Determine inherent risk before controls
- Document risk treatment (reduce, accept, transfer, avoid)
- Track remediation plans and due dates
- Review risks at least annually and upon major change

Risk Lifecycle

- Identify risks and impacted assets
- Analyze likelihood and impact
- Assign ownership and accountability
- Select appropriate treatment method
- Implement mitigation actions
- Monitor progress and reassess
- Document closure or acceptance
- Present in leadership and program reviews

8. Policies, Standards & Document Control

Effective SOC 2 compliance requires formal, approved, and regularly reviewed policy and standard documentation. These documents define the rules, control expectations, and operating procedures that govern security and compliance activities. Documentation must remain current, accessible, approved by appropriate leadership, and aligned with the organization's control environment and system description.

Policies and standards must support audit requirements and ensure consistent execution across teams, systems, and workflows. Document hygiene directly impacts audit readiness, control clarity, and workforce adoption.

Documentation Requirements

- Published security and compliance policies
- Supporting technology and operational standards
- Documented procedures and playbooks for key controls
- Mapping of policies to SOC 2 control requirements
- Centralized and controlled repository for documentation
- Training and acknowledgement for applicable personnel

Versioning & Approval Controls

- Version number and change history recorded
- Formal approval by designated authority (e.g., executive or CISO)
- Defined policy owner accountable for updates and accuracy
- Review and re-approval cycle at least annually
- Retention of prior versions for historical and audit use

Retention & Distribution

- Policies retained in an auditable system or repository
- Secure and controlled access to internal policies and procedures
- Distribution to relevant personnel and stakeholders
- Employee access ensured via workplace systems or knowledge bases
- Evidence of publication and workforce awareness maintained

9. Access Control & Identity Governance

Access control requirements ensure that only authorized personnel can access in-scope systems, environments, applications, and data. Controls must restrict access based on least privilege, job function, and business justification. Identity governance supports a repeatable method to provision, review, update, and remove access across systems supporting the SOC 2 scope.

These practices ensure traceability, accountability, and continuous control operation over identities, roles, and authentication. Proper access governance protects against unauthorized access, insider threats, and data misuse.

Core Access Control Practices

- Role-based access control and least-privilege enforcement
- Documented access provisioning and deprovisioning procedure
- MFA enforced across applicable systems and accounts
- Central identity provider and access management platform
- Segregation of duties for privileged or sensitive functions
- Access requests logged, reviewed, and approved
- Quarterly access reviews for in-scope systems
- Immediate access removal upon termination or role change
- Access logs retained to validate control execution

Expected Evidence

- Access request/approval records
- MFA enforcement artifacts
- User access review logs and confirmations
- Termination offboarding access removal evidence
- Privileged access list and validation
- Identity store audit logs

Identity & Access Lifecycle

- Request initiated through documented access channel
- Authorization granted based on role and business need
- Access provisioned and logged
- Periodic access reviews conducted
- Changes reviewed and updated as roles evolve
- Termination or role change initiates access removal
- Access removal validated and logged

10. Change Management & Secure SDLC

Change management ensures that modifications to systems, code, configurations, and infrastructure follow approved, documented, and validated processes. A secure SDLC supports structured design, development, testing, and release practices that maintain system confidentiality, integrity, and availability. These controls reduce risk associated with unauthorized or untested changes and support traceable, auditable software delivery.

This section establishes expectations for structured change implementation, documentation, review, separation of duties, and evidence generation across environments supporting SOC 2 scope. Controls apply to code changes, infrastructure configuration, and production deployment activities.

Core Change Management & SDLC Practices

- Documented change management policy and workflow
- Separation of duties between development and deployment functions
- Change requests logged and approved prior to implementation
- Peer review or automated review pipeline for code changes
- Testing and validation before production deployment
- Version control and audit trails for code and configuration
- Emergency change process with required post-implementation review
- Secure development guidance and security controls embedded in SDLC
- Vulnerability identification and remediation during development lifecycle

Expected Evidence

- Change tickets with documented approvals
- Pull request reviews and merge logs
- CI/CD pipeline logs and deployment records
- Test and validation results for releases
- Emergency change log with documented review
- Secure coding training records
- Version history for code and infrastructure as code artifacts

SDLC Lifecycle

- Requirements defined and documented
- Secure design review and architectural validation
- Code development in managed version control system
- Automated and manual testing performed
- Security checks (linting, dependency scanning, vulnerability scanning)
- Change approval documented
- Deployment executed via controlled pipeline
- Post-implementation validation performed and logged

11. System Operations & Monitoring

System operations and monitoring ensure that production environments remain stable, secure, and available. SOC 2 requires documented operational practices that maintain system health, detect anomalies, and support continuous oversight. These activities help validate that systems operate as intended and that issues are identified, escalated, and resolved in a timely manner.

Operational monitoring includes performance visibility, automated alerting, log review, and issue response. Evidence must demonstrate ongoing execution and traceability to defined operational procedures.

Core System Operations & Monitoring Practices

- Centralized infrastructure and application monitoring
- Logging and alerting across production systems
- Availability and resource utilization tracking
- Backup execution and validation
- Monitoring of system health, performance, and security events
- Routine review of operational dashboards and alerts
- Documented escalation and ticketing procedures for issues
- Incident logging and resolution tracking
- Operational runbooks for key components and services

Expected Evidence

- Monitoring dashboards or screen captures
- Alert logs and ticketing records
- Backup logs and restore test confirmations
- Runbooks and operational playbooks
- Documented issue escalations and resolutions
- Production log access and review documentation

Operational Monitoring Cycle

- Daily monitoring of production system health and alerts
- Weekly review of key operational metrics and exceptions
- Monthly backup and restore validation
- Quarterly review of operational runbooks and escalation processes
- Annual validation of monitoring and log coverage against scope

12. Incident Response & Business Continuity

Incident response and business continuity processes ensure the organization can detect, investigate, respond to, and recover from security incidents and operational disruptions. SOC 2 requires documented procedures, trained personnel, and evidence that the organization can maintain operations and protect customer commitments during adverse events. These processes reduce impact, support service availability, and protect the confidentiality and integrity of data.

This section defines expectations for incident handling, escalation, communication, and recovery procedures, along with continuity planning to support uninterrupted operational capabilities.

Core Incident Response & Business Continuity Practices

- Documented incident response plan and roles
- Defined incident severity levels and escalation pathways
- Monitoring and alerting to detect events and anomalies
- Ticketing and documentation of incidents and remediation actions
- Root cause analysis and corrective action activities
- Documented business continuity and disaster recovery plans
- Defined recovery priorities and RTO/RPO objectives
- Regular testing of IR and BC/DR procedures
- Secure communication paths for incident coordination
- Evidence of lessons-learned activities and plan updates

Expected Evidence

- Incident response plan and playbooks
- Incident logs and ticket records
- Escalation and communication documentation
- Root cause analyses and corrective actions
- Business continuity and disaster recovery plans
- DR test results and recovery validation
- Training or exercise participation records

Incident Response Lifecycle

- Event detection and log analysis
- Incident classification based on severity and scope
- Response and containment actions
- Evidence preservation and documentation
- Root cause analysis and corrective actions
- Communication to stakeholders when appropriate
- Closure with approvals and record retention

Business Continuity & Disaster Recovery Components

- Identification of critical systems and dependencies
- RTO (Recovery Time Objective) and RPO (Recovery Point Objective) established
- Backup coverage and integrity validation
- Continuity plans for personnel, communication, and operations
- DR site or recovery strategy defined
- Annual DR testing and updates based on results

13. Vendor & Subservice Provider Oversight

Third-party vendors and subservice providers supporting in-scope systems must be evaluated, monitored, and managed to ensure they meet security and compliance expectations. SOC 2 requires defined vendor governance, documented security review procedures, and evidence that vendors with access to in-scope data or environments are appropriately assessed and monitored. Vendor oversight strengthens trust assurances and mitigates supply-chain and dependency risks.

This section defines expectations for vendor selection, onboarding, review, monitoring, and removal—ensuring third-party activities do not introduce unacceptable risk to systems, data, or service delivery.

Core Vendor Oversight Practices

- Defined vendor management and security assessment procedures
- Risk assessment for third-party services handling in-scope functions
- SOC 2 or equivalent assurance review for critical providers
- Review of Complementary User Entity Controls (CUECs) and assumptions
- Collection and evaluation of bridge letters when applicable
- Vendor contractual requirements for security and confidentiality
- Documented monitoring and periodic reassessment
- Defined criteria for vendor acceptance and continuation
- Removal procedures for vendors no longer required or approved

Expected Evidence

- Vendor inventory and classification
- SOC 2 reports or equivalent assurance artifacts
- Bridge letters for coverage gaps
- Documented review notes for reports and CUECs
- Vendor risk ratings and remediation actions

- Signed contracts reflecting security obligations
- Evidence of reassessment and periodic review

Vendor Lifecycle

- **Identification & Scoping:** Evaluate vendor relevance to SOC 2 scope
- **Assessment:** Review SOC report or comparable assurance
- **Approval:** Confirm acceptance criteria and security requirements
- **Onboarding:** Grant access only after security checks completed
- **Monitoring & Reassessment:** Review reports and risk periodically
- **Termination:** Remove access and confirm secure offboarding

14. Logging, Monitoring & Continuous Testing

Logging and monitoring ensure that system activity, security-relevant events, and critical operational behaviors are captured and reviewed. SOC 2 requires consistent monitoring to detect unauthorized activity, identify anomalies, and support incident response and forensic investigation. Continuous testing validates that detection and monitoring controls operate as intended.

Logging and monitoring support data protection, system integrity, and audit readiness by identifying deviations from expected performance, security baselines, and compliance requirements. Evidence must demonstrate active oversight and review.

Core Logging & Monitoring Practices

- Centralized logging for production systems and services
- Coverage for authentication, access, privileged actions, and system events
- Monitoring dashboards for performance and security activity
- Alerting thresholds and notification workflows
- Defined responsibilities for log review and alert triage
- Correlation of events to detect anomalies and suspicious activity
- Retention aligned to SOC 2 requirements and business needs
- Continuous validation that monitoring controls operate effectively
- Routine tuning of log sources, detection logic, and alert thresholds

Expected Evidence

- Logging configuration and coverage documentation
- Alerting rules and escalation workflows
- Dashboard or SIEM screenshots
- Log review confirmations and ticket trails
- Exceptions and alert investigations recorded
- Evidence of periodic tuning and validation

Monitoring & Review Cadence

- **Daily:** Alert triage and priority log review
- **Weekly:** Broader log inspection and operational anomaly review
- **Monthly:** Configuration review and tuning updates
- **Quarterly:** Security detection validation and coverage assessment
- **Annually:** End-to-end control validation and audit alignment review

15. Data Protection & Encryption

Data protection controls ensure that information within the system remains secure throughout its lifecycle. SOC 2 requires safeguards that protect data confidentiality, integrity, and availability, supported by encryption, secure storage, and controlled access. Encryption in transit and at rest provides an added layer of security against unauthorized access or interception.

This section defines expected practices for securing data, implementing encryption standards, managing cryptographic materials, and demonstrating compliance through evidence. Controls support secure handling, processing, transmission, and disposal of customer and system data.

Core Data Protection Practices

- Defined data classification and handling requirements
- Encryption for data at rest using industry-standard ciphers
- Encryption for data in transit using secure protocols (e.g., TLS)
- Access control to encrypted systems and key-protected resources
- Secure configuration for databases and storage layers
- Separation of duties for encryption key access and management
- Monitoring and audit logging for sensitive data access
- Data loss prevention and leakage-monitoring safeguards where applicable
- Data disposal aligned to policy, regulatory, and contractual requirements

Expected Evidence

- Encryption policies and configuration documentation
- Key management procedures and access restrictions
- System-level security settings illustrating encryption enablement
- Logs for privileged data access events
- Secure disposal records and validation
- Data flow diagrams reflecting protected transport paths

Data Lifecycle

- **Collection:** Data received only through approved and secured channels
- **Storage:** Protected using encrypted storage technologies
- **Use:** Access monitored; privilege limited to authorized roles
- **Transmission:** Secured via encrypted transport protocols
- **Retention:** Retained only as long as necessary for services and commitments
- **Disposal:** Secure erasure and destruction of media and stored data

16. Availability Management & Resilience

Availability controls ensure that systems and services operate as intended and meet defined reliability, uptime, and continuity expectations. SOC 2 requires that systems supporting in-scope services be architected, monitored, and maintained to support continuous operations, minimize unplanned downtime, and ensure capacity for expected demand.

This section defines expectations for service availability, capacity planning, performance monitoring, fault-tolerance, and recovery processes that support operational resilience and service reliability.

Core Availability & Resilience Practices

- Defined availability objectives and performance benchmarks
- Infrastructure and application monitoring for capacity and load
- Automated scaling or reserved resource strategy where applicable
- Redundancy for critical system components and services
- Documented performance tuning and maintenance cycles
- Capacity forecasting and proactive resource planning
- Preventive maintenance program and patching schedules
- Uptime tracking and reporting to leadership
- Failover and recovery mechanisms implemented and tested

Expected Evidence

- Service availability policies and objectives
- Uptime dashboards and performance metrics
- Capacity planning documentation or forecast models
- Maintenance and patching logs
- Architecture diagrams showing redundancy and failover paths
- Test results for availability and resilience controls
- Communications documenting planned maintenance events

Availability & Resilience Lifecycle

- **Plan:** Define availability requirements and resource strategy
- **Monitor:** Track usage, performance, and operating thresholds
- **Scale:** Allocate resources to maintain performance and stability
- **Test:** Validate redundancy and failover functionality
- **Improve:** Optimize based on observed performance and test results

17. Training, Awareness & Workforce Compliance

Training and awareness ensure personnel understand their responsibilities in supporting security and SOC 2 compliance. A documented training program reinforces policies, secure practices, operational expectations, and role-specific responsibilities. SOC 2 requires annual training and appropriate onboarding procedures to ensure workforce readiness and compliance culture.

This section outlines expectations for continuous workforce education, role-based training, evidence maintenance, and structured reinforcement of secure and compliant behavior across the organization.

Core Training & Awareness Practices

- Formal security and compliance training program
- Required onboarding security and compliance orientation
- Annual security and SOC 2 awareness training
- Role-based training for personnel managing in-scope systems
- Documentation of policy review and acknowledgment
- Awareness campaigns to reinforce secure behavior
- Periodic updates based on evolving risks and control gaps
- Documentation of access to training content and completion status

Expected Evidence

- Training policy and defined curriculum
- New-hire training enrollment and completion logs
- Annual training completion records
- Role-specific training documentation where applicable
- Records of policy acknowledgments
- Awareness communications or campaign materials
- Tracking reports demonstrating training compliance

Training & Awareness Cycle

- **Onboarding:** New personnel receive foundational training and policy acknowledgment
- **Annual Certification:** Required training to maintain SOC 2 program compliance
- **Role-Based Training:** Targeted education for technical, privileged, or sensitive roles
- **Periodic Reinforcement:** Awareness reminders, guidelines, and threat updates
- **Documentation & Verification:** Training completion and tracking logs maintained

18. Monitoring, Internal QA & Continuous Improvement

Continuous monitoring and internal quality assurance validate that controls operate effectively throughout the year and that the SOC 2 program remains audit-ready. This includes evaluating control execution, verifying evidence quality, identifying gaps, and implementing improvement actions. Regular assessments ensure the environment aligns with Trust Services Criteria and support a mature, sustainable compliance function.

This section defines expectations for control monitoring, internal testing, documentation validation, and structured improvement cycles that reinforce readiness for external examination.

Core Monitoring & QA Practices

- Documented internal control testing plan
- Periodic review of key controls and evidence collection
- Verification that control owners fulfill assigned responsibilities
- Internal SOC 2 readiness assessments prior to external audit
- Documentation and tracking of control deficiencies
- Remediation plans and follow-up validation
- Review of security posture and program maturity
- Escalation of material issues to leadership

Expected Evidence

- Internal control testing documentation
- Evidence review reports and findings
- Remediation plans and status tracking
- Meeting notes or communications documenting review cycles
- Risk register updates tied to internal review outcomes
- Leadership reporting on program status and improvement activities

Continuous Improvement Cycle

- **Review:** Evaluate control performance and evidence quality
- **Analyze:** Identify gaps, emerging risks, and areas for enhancement
- **Remediate:** Implement corrective actions and validate results
- **Report:** Communicate findings to leadership and stakeholders
- **Refine:** Update policies, controls, and processes as required

19. Evidence Collection & Audit Readiness

Evidence collection validates the execution of controls and supports readiness for external examination. SOC 2 requires that control operation be demonstrated through reliable, dated, and verifiable documentation. A structured evidence program ensures records are timely, complete, and accessible to auditors, reducing audit friction and supporting program credibility.

Evidence must align to Trust Services Criteria, remain current, and be organized to support rapid retrieval during audits, reviews, and readiness checkpoints.

Core Evidence Collection Practices

- Maintain documented evidence requirements for each SOC 2 control
- Collect evidence at defined intervals (quarterly, annual, or event-driven)
- Validate evidence completeness, accuracy, and timeliness
- Assign ownership for evidence submission and approval
- Store evidence in a controlled and auditable repository
- Use naming conventions and labeling aligned to controls
- Secure storage and restricted access for sensitive evidence
- Maintain audit trail of evidence submission and review activities

Evidence Categories

- Security configurations and settings
- System access logs and reviews
- Change management tickets and approvals
- Incident response and recovery records
- Training and policy acknowledgement records
- Vendor SOC reports and monitoring artifacts
- Backup and restoration documentation
- Monitoring and alert triage records
- Risk and remediation records

Evidence Lifecycle

- **Collect:** Capture evidence at defined intervals or trigger events
- **Validate:** Confirm accuracy, completeness, and audit readiness
- **Store:** Retain in a centralized, controlled, and searchable repository
- **Retrieve:** Provide organized access during review or audit events

20. SOC 2 Type I vs. Type II Overview

SOC 2 examinations are conducted in two formats—Type I and Type II. Both evaluate the design of controls supporting Trust Services Criteria, but they differ in timing and depth of operating effectiveness assessment. Understanding these distinctions supports informed audit planning and alignment to organizational maturity and customer expectations.

This section clarifies the purpose, scope, and use cases for each examination type, along with key differences in preparation and evidence expectations.

SOC 2 Type I

Evaluates the design of controls at a point in time.

Primary Purpose

- Validate control structure and readiness
- Establish baseline compliance posture

Applicability

- Early-stage or first-time SOC participants
- Organizations building security maturity and evidence discipline
- Market-driven need to demonstrate initial assurance

Preparation Focus

- Documenting policies, procedures, roles, and governance
- Completing system description and control mappings
- Establishing evidence processes and control ownership

SOC 2 Type II

Evaluates design and operating effectiveness over a review period (typically 6–12 months).

Primary Purpose

- Demonstrate sustained compliance and control maturity

Applicability

- Organizations with established SOC compliance programs
- Enterprises requiring continuous trust and audit validation
- Customer-driven proof of ongoing operating effectiveness

Preparation Focus

- Evidence collection throughout the audit period
- Control execution traceable to calendars and owners
- Continued monitoring, remediation, and documentation

Key Differences

Area	Type I	Type II
Control Design Tested	✓	✓
Control Operating Effectiveness Tested	✕	✓
Audit Duration	Point-in-time	6–12 month performance period
Evidence Requirement	Immediate readiness	Evidence gathered over time
Use Case	First certification / readiness proof	Mature compliance demonstration

21. Definitions

This section provides key SOC 2 and security terminology used throughout the guide. These terms support clarity and consistency in governance, control execution, and audit preparation. Definitions reflect industry-standard meaning aligned with AICPA and Trust Services Criteria terminology.

Key Terms

Access Control
Methods used to restrict system access to authorized users and processes.

Audit Trail
Record of activity and events used to verify system actions and control execution.

Availability
Ensuring systems and data remain accessible to authorized users when needed.

Business Continuity
Plans and processes to ensure continued operation during disruption.

Change Management
Controlled process for modifying systems, applications, and configurations.

Confidentiality
Protection of data from unauthorized disclosure.

Control Owner
Individual responsible for executing and maintaining a designated control.

Control Evidence
Documentation demonstrating that a control operated as designed.

Data Flow
Movement of data across systems, environments, and storage points.

Encryption
Protection method converting data into unreadable form without a key.

Incident
Event that threatens confidentiality, integrity, or availability of systems or data.

Least Privilege
Limiting access rights to only what is required to perform job duties.

Monitoring
Review of security, operational, and system events to detect issues.

Privileged Access
Elevated permissions enabling administrative or sensitive system functions.

Remediation
Actions taken to correct control failures or security weaknesses.

Risk Assessment
Identification, evaluation, and prioritization of risks to systems and data.

Security Awareness Training
Workforce education on compliance responsibilities and secure behavior.

System Description
Formal documentation describing the services, architecture, and controls in scope.

Trust Services Criteria (TSC)
AICPA criteria defining requirements for SOC 2 compliance (Security, Availability, Processing Integrity, Confidentiality, Privacy).

Abbreviations

AICPA	American Institute of Certified Public Accountants
BC/DR	Business Continuity / Disaster Recovery
CI/CD	Continuous Integration / Continuous Deployment
CUECs	Complementary User Entity Controls
IAM	Identity and Access Management
IR	Incident Response
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
PII	Personally Identifiable Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLAs	Service-Level Agreements
SOC	System and Organization Controls

22. References

This section provides authoritative resources used to develop, operate, and validate SOC 2 compliance programs. Each reference includes a full, visible URL to ensure accessibility in offline or printed formats. These resources support interpretation of Trust Services Criteria, secure control implementation, industry best practices, and audit readiness.

AICPA & SOC 2 Standards

AICPA Trust Services Criteria
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/trustservicescriteria.html

AICPA SOC for Service Organizations — Guide
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html

AICPA SOC Examination Resources
https://www.aicpa.org/resources/article/system-and-organization-controls-soc-suite-of-services

Security & Risk Frameworks

NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

NIST Special Publication 800-53 Security and Privacy Controls
https://csrc.nist.gov/pubs/sp/800/53/r5/final

ISO/IEC 27001 Information Security Management
https://www.iso.org/standard/27001

ISO/IEC 27002 Information Security Controls
https://www.iso.org/standard/75652.html

Cloud Security Alliance (CSA) Cloud Controls Matrix
https://cloudsecurityalliance.org/research/cloud-controls-matrix

Secure Development & Application Security

OWASP Top Ten
https://owasp.org/www-project-top-ten/

OWASP ASVS
https://owasp.org/www-project-application-security-verification-standard/

Privacy & Data Protection

IAPP Privacy Resources
https://iapp.org/resources/

NIST Privacy Framework
https://www.nist.gov/privacy-framework

Cloud & Infrastructure

AWS SOC Reports & Compliance Resources
https://aws.amazon.com/compliance/soc-faqs/

Microsoft Azure Compliance
https://learn.microsoft.com/en-us/azure/compliance/offerings/

Google Cloud Compliance
https://cloud.google.com/security/compliance

Apptega

Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com