SOC 2 Type II Compliance

A Practical Guide for Security Teams

By Afaan Bilal • Principal Software Engineer, CISO • **afaan.dev**

Executive Summary

This comprehensive SOC 2 Type II compliance guide doc provides security teams with a practical roadmap for achieving and maintaining compliance. Unlike theoretical guides, this document focuses on implementable controls, evidence collection, and audit preparation based on real-world experience.

What You'll Get:

- 5-Phase compliance roadmap
- Detailed control mapping for all Trust Services Criteria
- Evidence collection templates
- Audit preparation checklist
- Implementation best practices

Phase 1: Pre-Audit Preparation

1

1.1 Define Audit Scope

- Identify all systems, networks, and applications in scope
- Document data flow diagrams for all in-scope systems
- Define user roles and access levels
- List third-party vendors and service providers
- Determine which Trust Services Criteria apply:
  - Security (Common Criteria - Required)
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy

2

1.2 Gap Assessment

- Conduct current state vs. required controls analysis
- Document all identified gaps
- Prioritize gaps by risk level
- Create remediation timeline
- Assign ownership for each gap

3

1.3 Establish Governance Framework

- Define compliance team roles and responsibilities
- Establish steering committee for oversight
- Create communication plan for stakeholders
- Set up regular compliance review cadence
- Document escalation procedures

Phase 2: Security Controls Implementation

2.1 Access Management (CC6.1, CC6.2, CC6.7, CC6.8)

Formal User Access

Provisioning & Deprovisioning

Least Privilege

Enforced for all systems

Multi-Factor Auth (MFA)

- Remote & Admin access
- Critical systems
- Third-party vendors

Access Reviews

Regular reviews (quarterly/semi-annual)

Password Policies

- 14+ chars, complexity
- 90-day rotation
- History enforcement

2.2 Network Security (CC6.1, CC6.4)

Network Segmentation

Implemented & enforced

Firewall Reviews

Quarterly rule audits

IDS/IPS

Intrusion detection/prevention systems

VPN Encryption

For remote access

Traffic Monitoring

Proactive network surveillance

Wireless Security

Robust controls in place

2.3 Data Protection (CC6.1, CC6.2, CC6.11)

Data Classification

Public, Internal, Confidential, Restricted

Encryption At Rest

AES-256 minimum

Encryption In Transit

TLS 1.3+ protocols

Prefer Post-Quantum (optional)

DLP Controls

Data loss prevention systems

Backup Security

Encrypted & secure storage

Data Policies

Retention & deletion guidelines

2.4 System Development & Maintenance (CC7.1, CC8.1)

Secure SDLC

Integrated security lifecycle

Code Reviews

Thorough review processes

SAST/DAST

Static & dynamic security testing

Third-Party Assessments

Software security evaluations

Change Management

Controlled procedures

QA Security Testing

Integrated security checks

Phase 3: Security Operations

1

Incident Management (CC3.1, CC4.4)

- Incident response plan development
- Incident classification and severity levels
- 24/7 monitoring and alerting
- Incident response team (IRT) with defined roles
- Regular incident response testing (quarterly)
- Post-incident review process
- Threat intelligence program

2

Vulnerability Management (CC4.1, CC8.1)

- Quarterly vulnerability scanning of all systems
- Patch management processes:
  - Critical patches: 7 days
  - High severity: 30 days
  - Medium severity: 90 days
  - Low severity: 180 days
- Penetration testing (annual, plus after major changes)
- Vulnerability risk scoring and prioritization
- Asset inventory management

3

Monitoring & Logging (CC6.6, CC6.10)

- Centralized log collection (SIEM)
- Log retention policy (minimum 90 days, preferably 1 year)
- Real-time monitoring of:
  - Failed authentication attempts
  - Administrative actions
  - Configuration changes
  - Data access patterns
- Alert tuning to reduce false positives
- Log integrity controls

Phase 4: Trust Services Criteria Implementation

4.1 Security

Control Environment

- Information security policies
- Board-level security oversight
- Annual security awareness training
- Security communication programs
- Annual risk assessment methodology

Communication

- Incident reporting procedures
- Security awareness channels
- Vendor security requirements
- Customer security responsibilities

Risk Assessment

- Annual comprehensive risk assessment
- System-specific risk assessments
- Business impact analysis
- Risk acceptance procedures

Risk Mitigation

- Control implementation for risks
- Control testing procedures
- Continuous control monitoring
- Defect identification & remediation

Monitoring

- Continuous control monitoring
- Control effectiveness measurements
- Periodic control testing
- Defect identification & remediation

4.2 Availability

Planning & Testing

- System availability targets
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Annual BCP/DRP testing

Redundancy

- Power redundancy (UPS, generators)
- Network redundancy (multiple ISPs)
- System redundancy (load balancers)

Metrics & Monitoring

- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Availability monitoring/reporting
- Incident resolution SLAs

4.3 Processing Integrity

Data Accuracy

- Input validation controls
- Processing accuracy monitoring
- Output verification procedures
- Error handling & correction
- Data reconciliation

Operational Controls

- Transaction logging & audit trails
- Change management with testing

4.4 Confidentiality

Data Protection

- Confidentiality requirements
- Data encryption implementation
- Access controls for confidential data
- Data classification labels
- Secure transmission methods
- Data disposal procedures
- Third-party agreements

4.5 Privacy

Privacy Management

- Privacy policies
- Personal data inventory
- Privacy impact assessments
- Data subject rights procedures
- Consent management processes
- Privacy breach procedures
- Regulatory compliance monitoring

Phase 5: Audit Preparation

1

5.1 Documentation Requirements

- All policies formally documented and approved
- Procedures documented with step-by-step instructions
- Evidence collection procedures established
- Document version control implemented
- Document retention policy enforced

2

5.2 Evidence Collection

For each control, collect:

- Policy documents
- Procedure documentation
- System configurations
- Review meeting minutes
- Training records
- Incident reports
- Monitoring reports
- Test results
- Vendor documentation
- Change tickets

3

5.3 Audit Readiness Checklist

- Gap analysis completed (30-60 days before audit start)
- All controls implemented (60 days before audit start)
- Evidence repository organized (45 days before audit start)
- Staff interviews prepared (30 days before audit start)
- Walkthrough scripts ready (30 days before audit start)
- Mock audit completed (30 days before audit start)
- Audit scope final agreed (30 days before audit start)

Evidence Collection

Monthly Evidence

- Access review reports
- Change management records
- Security training completion reports
- Vulnerability scan results
- Backup verification logs

Quarterly Evidence

- Privileged access reviews
- Firewall rule reviews
- Incident response testing results
- Risk assessment updates
- Vendor risk assessments

Annual Evidence

- Full risk assessment
- Penetration test results
- BCP/DRP test results
- Security awareness training records
- Policy review approvals

Quick Start Implementation Timeline

1

Week 1-2: Foundation

- Form compliance team
- Define audit scope
- Conduct initial gap assessment

2

Week 3-8: Control Implementation

- Implement critical security controls
- Develop policies and procedures
- Begin evidence collection

3

Week 9-12: Testing & Refinement

- Conduct internal testing
- Perform mock audit
- Address identified gaps

4

Week 13-16: Final Preparation

- Complete evidence repository
- Train staff for interviews
- Final audit readiness

In Audit Window (Type II)

The audit window is a critical phase where your organization's security and compliance posture is rigorously examined by an independent auditor, typically spanning 3 to 12 months. Success hinges on meticulous preparation, transparent communication, and maintaining the operational integrity of your established controls.

- **Audit Kick-off & Scope Confirmation**

  Begin with an official kick-off meeting to introduce personnel, confirm audit scope, establish communication protocols, and agree on timelines. Ensure all stakeholders understand their roles and responsibilities during this intensive period.

- **Evidence Submission & Review**

  Systematically submit all collected evidence, such as policy documents, configuration records, and activity logs. Auditors will review this for completeness and alignment with SOC 2 criteria, and you should be prepared for follow-up questions.

- **Personnel Interviews & Control Walkthroughs**

  Auditors will interview key personnel across departments to verify understanding and adherence to controls. Staff will demonstrate the actual operation of critical security processes, offering a qualitative assessment of control effectiveness.

- **Prompt Inquiry Response**

  Auditors will frequently request clarification or additional evidence. Establish an efficient internal process for prompt and accurate responses to avoid delays. Maintain a detailed log of all requests and responses.

- **Continuous Control Operation**

  All security controls must operate effectively and consistently throughout the audit period. Any lapses or significant changes without auditor awareness can negatively impact the outcome. Continue regular monitoring and incident response activities.

- **Regular Debriefs & Issue Resolution**

  Schedule regular check-ins with the audit team to track progress, discuss preliminary findings, and proactively address potential issues. Early identification and resolution can prevent findings from escalating into significant audit exceptions.

By actively managing these phases, organizations can navigate the SOC 2 Type II audit window effectively, leading to a successful report that builds trust with clients and partners.

Success Metrics

Key Performance Indicators:

Critical controls implemented	**Evidence collected 30 days before audit**
100%	95%
High-risk vulnerabilities	**Staff completion of security training**
0	100%
Quarterly access review completion rate	
95%	

Common Pitfalls to Avoid

1	**Starting too late** Begin 6+ months before audit
2	**Insufficient documentation** Document everything
3	**Evidence collection rush** Collect continuously
4	**Staff unpreparedness** Train and brief all participants
5	**Scope creep** Keep audit scope focused and agreed

Next Steps

Immediate Actions (This Week):

1	2
Form your compliance team	Define your audit scope
3	**4**
Schedule your initial gap assessment	Set up your evidence repository

Schedule a Consultation:

Need expert guidance on your SOC 2 journey? As a CISO who's led successful SOC 2 Type II certifications, I can help streamline your compliance process.

https://afaan.dev **hello@afaan.dev**

About the Author: *Afaan Bilal is a Principal Software Engineer and CISO with extensive experience in building secure, SOC 2 Type II certified SaaS platforms serving millions. He combines technical expertise with practical security leadership to help organizations achieve compliance efficiently.*

This checklist is based on real-world experience implementing SOC 2 Type II controls. Feel free to adapt it to your specific needs while maintaining the core principles outlined above.

Last Updated: February 2026
Version: 1.0

Did you find this checklist helpful? Share it with your team and connect with me on **LinkedIn** for more security insights.