SOC 2 Type II Audit Readiness Toolkit 2026

Gap checklist, evidence matrix, policy templates, and control checklists for CISOs, CTOs, and compliance teams preparing for their SOC 2 Type II audit observation window.

47
controls across 5 Trust Services Criteria areas

WHAT IS IN THIS TOOLKIT?

QUICK START

How to Use This Toolkit

This toolkit helps you run an internal SOC 2 Type II readiness simulation — identifying control gaps, missing evidence, and process weaknesses before your auditor shows up. Use it as a self-assessment tool or as a work-back planning document for your audit timeline.

1 **Complete the Gap Checklist (Pages 4–6)**
Work through all 47 control items across CC1–CC9. Mark each one: Implemented + Evidence in Hand, Implemented but Evidence Weak, Not Implemented. This is your gap register.

2 **Map Evidence Gaps (Page 7)**
For every item marked "Evidence Weak" or "Not Implemented," cross-reference the evidence matrix. Identify the specific artifact you need, who owns it, and how far back it needs to cover (start of observation window).

3 **Edit the Policy Templates (Pages 8–9)**
The five policy templates are ready to use as-is for most SaaS companies, or adapt them to your environment. Key requirement: policies must be dated within the observation window — auditors look for policies that predate the window start.

4 **Score Controls (Page 12)**
Rate each control across three dimensions: design effectiveness (1–5), operating effectiveness (1–5), and evidence quality (1–5). Aggregate scores below 10 indicate a control that needs attention before audit.

5 **Build Your 90-Day Plan (Page 13)**
Use the month-by-month checklist on Page 13. Month 1: close the highest-severity gaps. Month 2: operationalize monitoring controls. Month 3: verify all evidence is organized and accessible for the audit team.

6 **Know What Auditors Want (Page 11)**
67% of first-time SOC 2 Type II audits find gaps in access review evidence, change management logs, and vulnerability scan reviews. Review Page 11 before your audit to understand where organizations fail and how to avoid it.

> **OBSERVATION WINDOW**
>
> Most organizations use a 6-month or 12-month observation window. If yours is 6 months and you are 4 months in, you have 2 months left to operationalize controls AND document them. Starting now is better than waiting.

TRUST SERVICES CRITERIA

Five Trust Services Criteria — Know Your Scope

Your audit report will specify which TSCs are in scope. Most SaaS companies include Security, Availability, and Confidentiality. Processing Integrity applies only to payment processors and data processing services. Privacy applies only when you handle PII under a privacy framework.

SECURITY — Common Criteria (CC1–CC9) — Required for all SOC 2 audits

The Common Criteria cover the control environment, communication and information, risk assessment, monitoring, and specific security controls. CC1: Control Environment. CC2: Communication and Information. CC3: Risk Assessment. CC4: Monitoring Activities. CC5: Control Activities. CC6: Logical and Physical Access Controls. CC7: System Operations. CC8: Change Management. CC9: Risk Mitigation.

Scope: Required for all SOC 2 Type II audits. No exceptions.

AVAILABILITY — A1.1, A1.2, A1.3

Commitment to availability SLAs. Requires BCP/DR documentation, system resilience controls, and incident response uptime commitments. Covers: current uptime SLAs, environmental controls, BCP and DR plans, recovery procedures, and monitoring.

Scope: Common for SaaS, cloud hosting, and any company that offers uptime guarantees.

CONFIDENTIALITY — C1.1, C1.2

Controls for identifying and protecting confidential information. Covers: data classification policy, access restrictions, encryption at rest and in transit, secure disposal procedures, and monitoring for unauthorized disclosure.

Scope: Common for SaaS, financial services, healthcare, and any company handling trade secrets, M&A data, or sensitive financial information.

PROCESSING INTEGRITY — PI1.1 through PI1.5 — Conditional

Accurate, complete, and timely processing. Covers: data validation, error detection and correction, processing monitoring, and accurate file processing. Requires documented processing agreements and monitoring systems.

Scope: In scope primarily for payment processors, payroll processors, financial data clearinghouses, and data processing services.

PRIVACY — P1 through P8 — Conditional

Privacy Notice, Choice & Consent, Collection, Use, Retention, Disclosure, Access, and Quality. Requires documented privacy notice, consumer consent mechanisms, data retention schedules, and processes for handling privacy complaints.

Scope: In scope when you handle PII under a privacy framework (GDPR, CCPA, CalOPPA). Requires formal privacy risk assessment.

GAP CHECKLIST — CC1 THROUGH CC3

47-Control SOC 2 Type II Gap Checklist

For each control: (A) Implemented + Evidence in Hand (green) / (B) Implemented, Evidence Weak (yellow) / (C) Not Implemented (red) / (D) Not Applicable

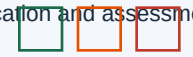
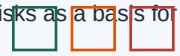
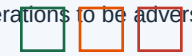
CC1 — Control Environment

CC1.1	Board or audit committee has oversight of the control environment, including security risk assessment and control monitoring.	
CC1.2	Management establishes structures, reporting lines, and appropriate authorities and responsibilities for the achievement of security objectives.	
CC1.3	Management communicates internally about security objectives, including expectations of integrity, ethical values, and competence.	
CC1.4	Board and management hold individuals accountable for their internal control responsibilities.	

CC2 — Communication and Information

CC2.1	Management communicates internally about the quality, accuracy, and completeness of financial and operational data.	
CC2.2	Management communicates externally about matters affecting the functioning of internal control.	
CC2.3	Management communicates internally about the security program, including reporting deficiencies and ensuring accountability.	

CC3 — Risk Assessment

CC3.1	Management specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.2	Management identifies risks to the achievement of objectives and analyzes risks as a basis for determining how risks should be managed.	
CC3.3	Management evaluates the likelihood and magnitude of the potential for operations to be adversely impacted by security threats.	
CC4.1	Management selects and monitors controls to mitigate security risks to acceptable levels, including risks from vendors and sub-processors.	

GAP CHECKLIST — CC4 THROUGH CC6

CC4 — Monitoring Activities

CC4.1	Management selects and develops ongoing evaluations to ascertain whether control components are present and functioning. (Note: labeled CC4.1 in some frameworks — maps to CC3.4)
CC4.2	Management evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action.

CC5 — Control Activities

CC5.1	Management selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	Management deploys control activities through policies that establish what should be done and procedures that establish how it should be done.
CC5.3	Entity uses technical controls to enforce access restrictions and to prevent or detect unauthorized or inappropriate activity.

CC6 — Logical and Physical Access Controls

CC6.1	Prior to issuing system credentials, management registers and authorizes new users according to documented onboarding procedures.
CC6.2	Management removes access to protected information and information systems when appropriate, following documented offboarding procedures.
CC6.3	Management implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software.
CC6.4	Management restricts physical access to facilities, protects documents and media from unauthorized access, and properly disposes of documents and media.
CC6.5	Management implements logical access security measures to protect against threats from external sources.
CC6.6	Management assigns user credentials and roles based on documented access control policies and the principle of least privilege.

GAP CHECKLIST — CC7 THROUGH CC9

CC7 — System Operations	
CC7.1	Management implements controls to monitor compliance with availability commitments and system availability SLAs.
CC7.2	Management performs vulnerability scans and penetration tests and takes action to remediate identified findings.
CC7.3	Management monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors.

CC8 — Change Management	
CC8.1	Management authorizes, designs, develops, configures, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet objectives.
CC8.2	Management prohibits unauthorized changes and manages changes to existing software, hardware, and infrastructure to meet objectives.
CC8.3	Management plans for and executes changes to mitigate risks from environmental changes, new technologies, and changing business needs.

CC9 — Risk Mitigation	
CC9.1	Management identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	Management identifies, selects, and develops risk mitigation activities for risks arising from the use of vendors and business partners.
CC9.3	Management implements processes to identify and respond to security incidents, communicate with affected parties, and coordinate with auditors.
CC9.4	Management has business continuity and disaster recovery plans in place that are tested and maintained, with designated backup sites and alternative processing capabilities.

EVIDENCE MATRIX

Evidence Matrix — What Auditors Want to See Per Control

For each control, auditors look for: (1) a policy or procedure describing the control, (2) evidence that the control operated throughout the observation window, (3) consistency — not a one-time snapshot. The most common failure mode is having a policy but no evidence it was followed.

Control	Evidence Required	Evidence Owner
CC6.1 — User Provisioning	HR system records + ticketing system provisioning tickets + access review logs	IT Ops / HR
CC6.2 — User Deprovisioning	Ticketing system termination tickets + access review logs + last-login timestamps	IT Ops / HR
CC6.3 — Anti-Malware	EDR console reports + malware detection logs + incident response records	Security / IT
CC6.4 — Physical Access	Badge access logs + visitor log + CCTV retention records + media disposal certificates	Facilities / Security
CC6.5 — Logical Access Security	Firewall logs + VPN connection logs + MFA enrollment report + access review	IT Ops / Security
CC6.6 — Access Reviews	Quarterly access review sign-off + evidence of follow-up on terminated/excessive access	IT Ops / Manager
CC7.1 — Availability Monitoring	Uptime monitoring dashboards + incident reports + SLA breach records	IT Ops / DevOps
CC7.2 — Vulnerability Management	Quarterly scan reports + penetration test report + remediation tracking log	Security / IT
CC7.3 — Anomaly Detection	SIEM dashboards + security alert logs + incident response records	Security Ops
CC8.1 — Change Authorization	Change management tickets + approval records + test results + rollback documentation	IT / DevOps
CC8.2 — Unauthorized Change Prevention	Change management system logs + emergency change approval records	IT Ops
CC9.2 — Vendor Risk	Vendor security questionnaires + SOC 2 reports on file + contractual security requirements	Security / Procurement
CC9.3 — Incident Response	IR plan + tabletop exercise records + incident response logs + post-incident reviews	Security / Management

EVIDENCE DATE MATTERS

Evidence must be from the observation window — not just before or after. If your observation window started January 1, any policy dated December 31 of the prior year is fine. But your access review logs, change logs, and vulnerability scan records must cover January 1 through the audit date.

POLICY TEMPLATES

Five Ready-to-Edit Policy Templates

Each template is ready to use as-is for most SaaS organizations, or adapt to your specific environment. All policies should be: (1) signed and dated by management, (2) version-controlled, (3) communicated to relevant staff. Auditors want to see policies that predate the observation window start.

1. Information Security Policy

Applies to: All employees, contractors, and third parties with access to company systems.

- Statement of security objectives and commitment to protecting confidentiality, integrity, and availability
- Acceptable use policy for company systems, devices, and data
- Password and authentication requirements (minimum length, MFA, complexity)
- Data classification: Public, Internal, Confidential, Restricted
- Acceptable encryption standards: AES-256 at rest, TLS 1.2+ in transit
- Acceptable use of cloud services and personal devices (BYOD policy)
- Security training requirements (annual minimum for all staff)
- Disciplinary procedures for policy violations

2. Access Control Policy

Applies to: IT Ops, HR, and all system owners responsible for access provisioning and removal.

- User provisioning: role-based access, least privilege, documented approval via ticketing system
- User deprovisioning: immediate removal of access upon termination or role change (within 24 hours)
- Access reviews: quarterly review of all privileged accounts, semi-annual review of standard accounts
- MFA requirements: mandatory for all remote access, all cloud services, all privileged accounts
- Password policy: minimum 12 characters, complexity requirements, 90-day rotation for privileged accounts
- Service account management: separate credentials, no shared accounts, quarterly rotation
- Shared account prohibition: no sharing of credentials for any system

3. Change Management Policy

Applies to: All infrastructure, application, and configuration changes to production systems.

- All production changes require documented approval through a change management system
- Changes classified as Standard, Normal, or Emergency with corresponding approval requirements
- Test environment: all changes tested in non-production environment before production deployment
- Rollback procedures: documented rollback plan required for all changes to critical systems
- Post-implementation review: verification of change success within 24 hours of deployment
- Emergency changes: documented and reviewed within 48 hours post-deployment
- Change advisory board (CAB) for high-risk changes affecting availability SLAs

POLICY TEMPLATES (CONTINUED)

4. Incident Response Policy

Applies to: Security team, IT Ops, and all personnel who may respond to security incidents.

- Incident classification: Critical, High, Medium, Low with response time SLAs per tier
- Detection methods: SIEM alerts, EDR alerts, user-reported incidents, vulnerability scan findings
- Containment procedures: immediate containment steps per incident type (malware, credential compromise, data exfil)
- Evidence preservation: imaging, log preservation, chain of custody documentation
- Notification requirements: internal escalation, affected customer notification, regulatory reporting within required timeframes
- Post-incident review: root cause analysis within 5 business days of incident closure
- Contact list: CISO, legal counsel, external forensics firm, cyber insurance carrier

5. Vendor Risk Policy

Applies to: Procurement, Security, and any team that engages third-party vendors with access to systems or data.

- Vendor classification: Critical, Important, Standard based on data access and system integration
- Security questionnaire: required for all vendors with access to Confidential or Restricted data
- Contractual requirements: all Critical vendors require audit rights, breach notification SLA, and DPA or BAA as applicable
- Annual review: all Critical and Important vendors reviewed annually; questionnaires refreshed
- Sub-processor disclosure: vendors must provide sub-processor list and notify of material changes
- Termination procedures: data return and destruction documented within 30 days of contract termination
- Evidence retention: SOC 2 reports, questionnaire responses, and contracts retained for audit period

CONTROL CHECKLISTS

Control Checklists — CC1 through CC9

Use these checklists during your internal audit simulation. Check each item, note the evidence, and flag any gaps.

CC6 — Logical & Physical Access Controls

- [ ] User provisioning process is documented and operating — HR ticketing system records exist
- [ ] User deprovisioning removes all access within 24 hours of termination — access review logs confirm
- [ ] MFA enforced for all remote access (VPN, cloud services) — MFA enrollment reports on file
- [ ] Phishing-resistant MFA (FIDO2) deployed for privileged accounts — enrollment records confirm
- [ ] Quarterly access reviews completed and signed off — review documentation retained
- [ ] Physical access logs maintained and reviewed — badge access records available for audit period
- [ ] Laptop encryption (FileVault / BitLocker) enabled and MDM enrolled — MDM console reports available
- [ ] No shared accounts for any production system — evidence: access control policy + audit trail review

CC7 — System Operations

- [ ] Uptime monitoring active — dashboards available covering the full observation window
- [ ] Vulnerability scans run at least quarterly — reports retained and findings tracked to remediation
- [ ] Penetration test completed within the observation window — executive summary on file
- [ ] Critical CVE patches applied within SLA (30 days for CVSS 9.0+) — patch log confirms
- [ ] Security event monitoring (SIEM) active — alert logs covering the observation window available
- [ ] SIEM alerts reviewed and responded to — evidence: ticket records for security alerts

CC8 — Change Management

- [ ] All production changes authorized through change management system — change log covers full window

- ☐ Emergency changes documented and reviewed within 48 hours — emergency change log available
- ☐ Change management tickets show: description, approval, testing, rollback plan, post-change verification
- ☐ No unauthorized changes to production (no direct commits to main/production branches without CR)

CC9 — Risk Mitigation

- ☐ IR plan documented, dated, and shared with relevant personnel — IR plan date predates observation window
- ☐ Tabletop exercise completed within the last 12 months — exercise records on file
- ☐ BCP/DR plan documented and tested — test results available
- ☐ Vendor security questionnaires on file for all Critical and Important vendors — current year
- ☐ Vendor contracts include breach notification SLA and audit rights — contract review confirms

TOP 10 FINDINGS

Top 10 Reasons Organizations Receive Qualified SOC 2 Opinions

These findings account for the majority of qualified opinions and corrective action requests in SOC 2 Type II audits. Each one is preventable with proper evidence collection.

1. Incomplete Access Review Evidence

Access reviews were performed, but documentation was not retained or not signed. Auditors require evidence of who reviewed, when, and what action was taken on exceptions.

2. Change Management Logs Incomplete

Change tickets exist but lack approval records, test results, or rollback documentation. Emergency changes lack post-incident review.

3. Vulnerability Scan Results Not Reviewed

Scans were run, but there is no evidence that findings were reviewed, triaged, or remediated within the SLA. Auditors look for a closed loop.

4. Security Training Not Tracked in Audit-Ready System

Training was completed but records are in an ad-hoc spreadsheet or email, not a system that produces a verifiable completion report.

5. Vendor Questionnaire Evidence Missing or Stale

Questionnaires were sent but responses not received, not signed, or not retained in a centralized system. Critical vendors missing current-year questionnaire.

6. Incident Response Test Records Missing

IR plan exists but there is no record of a tabletop exercise or test in the observation window. No evidence the team practiced the plan.

7. Policies Dated After Observation Window Started

Policies were created mid-window. Auditors look for policies that predate the window. A policy created in March cannot cover January–June observations.

8. BCP/DR Tested But Not Documented

DR plan was tested but results were not documented. Without a test report, auditors cannot confirm the plan was actually executed.

9. Logical Access Evidence Gap for Service Accounts

User access is reviewed but service accounts and API keys lack periodic review. CC6.5 requires monitoring of all access, not just human users.

10. Segregation of Duties Not Documented

No evidence of review for segregation of duties conflicts — e.g., developers with production access, or users with ability to both request and approve changes.

SCORING RUBRIC

Control Scoring Rubric — Design × Operating × Evidence

Rate each control across three dimensions. Aggregate score determines your readiness status. Any control scoring below 8 requires immediate remediation before your observation window closes.

Dimension	What to Score	Scale
Operating Effectiveness	Was the control followed consistently throughout the observation window?	1 (Not operating) !’ 5 (Consistently operating)
Evidence Quality	Can you demonstrate operating effectiveness with auditable evidence?	1 (No evidence) !’ 5 (Complete, organized, accessible)

SCORE INTERPRETATION

13–15 Audit Ready	Control is fully implemented with strong evidence. Maintain documentation throughout the observation window.
9–12 Minor Gaps	Control operates but evidence may need strengthening. Address within 30 days.
5–8 Significant Gap	Control has material gaps. Requires remediation plan before renewal. Do not proceed to audit without addressing.
1–4 Control Failure	Control is missing or not operating. Must be remediated before the observation window closes. Escalate to leadership.

90-DAY PLAN

90-Day SOC 2 Type II Readiness Plan

Use this as a work-back schedule from your audit date. Adjust month boundaries based on when your observation window closes.

MONTH 1 — Gap Closure

- [ ] Complete gap checklist for all 47 controls — document evidence owner and gap severity
- [ ] Review top 10 audit findings (Page 11) and confirm evidence for each in your environment
- [ ] Close any CC6 (access control) gaps — ensure access reviews are documented and signed
- [ ] Close change management gaps — ensure all production changes have approval + test records
- [ ] Confirm vulnerability scan results were reviewed and triaged (last 3 months minimum)
- [ ] Verify all security training completion records are in an auditable system
- [ ] Map all Critical and Important vendor evidence to the evidence matrix (Page 7)
- [ ] Review policies — confirm all 5 policy templates are signed, dated, and version-controlled
- [ ] Flag any control with an aggregate score below 8 and assign an owner for closure

MONTH 2 — Operationalize Monitoring

- [ ] Confirm SIEM monitoring covers the full observation window — export logs covering January 1 through current date
- [ ] Run quarterly access review and retain signed evidence — this is the most commonly missed item
- [ ] Ensure MFA enrollment report is current — export from your IdP (Okta, Azure AD, Google Workspace)
- [ ] Confirm patch management logs cover the full observation window — no gaps in coverage
- [ ] Conduct a tabletop incident response exercise if not done in the last 12 months
- [ ] Review and update IR plan if business or system changes since last version
- [ ] Confirm BCP/DR test results are documented and retained
- [ ] Collect all evidence into a shared, organized audit evidence folder — auditor will request access

MONTH 3 — Final Verification

- [ ] Run final gap checklist walk-through — confirm all items rated green or addressed
- [ ] Verify all evidence is in the audit evidence folder: access review logs, change logs, scan reports, training records, vendor questionnaires, policy documents
- [ ] Confirm observation window start date and back-anchor all policies to that date or earlier
- [ ] Conduct executive walk-through of evidence with audit team before auditor arrives (if possible)
- [ ] Brief all personnel who will be interviewed by auditors on the control narratives and their responsibilities
- [ ] Confirm backup site and DR capabilities are tested and documented
- [ ] Final review of segregation of duties — no conflicts in production access
- [ ] Confirm cyber insurance documentation is available (policy, coverage, recent claims history)

LIVE TRAINING

Put This Into Practice — SOC 2 Type II Live Training

The toolkit identifies where your gaps are. SecurEveryone live training shows your team how to build the evidence — running access reviews, documenting change management, executing IR tabletop exercises, and preparing for the auditor interview. Organizations that use both the toolkit and live training have a significantly higher rate of clean opinions on first audit.

PERSONAL

$299

1 session · 1 hour

Access review process training: how to run, document, and retain evidence for quarterly access reviews that satisfy CC6.5.

Best for: IT admins, compliance leads, security tea

- Access review process walk-through
- Evidence documentation standards
- Quarterly review cadence setup
- CC6.5 control narrative training
- Certificate of completion

EXECUTIVE

$899

1 session · 90 minutes

SOC 2 Type II readiness tabletop: walk through the top 10 audit findings, simulate auditor interview questions, and build your evidence story.

Best for: CISOs, CTOs, compliance officers, and fo

- 90-minute facilitated session
- Top 10 findings walk-through
- Auditor interview simulation
- Evidence organization review
- IR plan tabletop (CC9.3)
- Post-session written summary

BUSINESS

Custom

Unlimited users · 12 months

Full SOC 2 Type II readiness program: quarterly access reviews, change management documentation, IR tabletop exercises, and ongoing readiness support.

Best for: SaaS companies with complex environments or multiple TSCs in audit scope

- Unlimited live sessions for 12 months
- Quarterly access review facilitation
- Change management process documentation
- IR tabletop exercises (quarterly)
- Full CC1–CC9 control narrative support
- Auditor readiness interview prep
- Post-session audit evidence summaries

BOOK A SOC 2 STRATEGY SESSION

Schedule your Executive session at secureveryone.com/book. Use code SOC2READINESS for a $100 discount on your first session.

SecurEveryone LLC · 1201 North Orange Street, Wilmington, DE 19801 · +1 (302) 212-0500 · info@secureveryone.com