Buyers Guide

SOC 2 Identity-First Readiness Checklist

Learn what SOC 2 compliance really means for SaaS companies—why trust drives revenue, how audits work, and how to become audit-ready without chaos.

Operational checklist with owners & evidence

How to use this template

Assign an Owner for every control area

Check items only when they are true in production, not “planned”

Link evidence directly (Notion pages, screenshots, exports, tools)

This template should stay live year-round, not just before audits

Control Metadata

SOC Scope: Security (Common Criteria)
Audit Type: SOC 2 Type II
Observation Period: Start Date → End Date
Primary Auditor: CPA Firm Name
Last Reviewed: Date

1. Identity Inventory & Ownership

SOC 2 CC Mapping:

- CC1.2 – Assignment of responsibility
- CC2.2 – Information and communication
- CC6.1 – Logical access security

Control Objective: All identities are known, owned, and purpose-bound.
Control Owner: @Owner

Evidence Location: Identity inventory / IAM dashboard

- All human identities inventoried (employees, contractors, interns)
- All non-human identities inventoried (service accounts, API tokens, bots)
- Every identity has a named owner
- Every identity has a documented business purpose
- No shared user accounts without approved exception
- Identity sources of truth defined (HRIS, IdP, directories)
- Inventory continuously maintained

Notes / Exceptions:

- ...

2. Authentication & Baseline Access Controls

SOC 2 CC Mapping:

- CC6.1 – Logical access restriction
- CC6.6 – Authentication mechanisms

Control Objective: Strong authentication is consistently enforced.
Control Owner: @Owner

Evidence Location: IdP configuration / MFA policies

- MFA enforced for all users
- MFA enforced for all privileged users
- MFA exceptions documented and time-bound
- Password policies meet security standards
- SSO enforced for critical SaaS and cloud systems
- Production access requires strong authentication
- Privileged access requires step-up authentication or approval

Notes / Exceptions:

- ...

3. Joiner–Mover–Leaver (JML) Lifecycle Management

SOC 2 CC Mapping:

- CC6.2 – User provisioning
- CC6.3 – User access modification
- CC6.1 – Access restriction

3.1 Joiner (Onboarding)

Owner: @Owner
Evidence: Onboarding workflows / logs

- Standardized onboarding workflow
- Role- or attribute-based access assignment
- Access granted only after start date
- All access grants are timestamped

Notes / Exceptions:

- ...

3.2 Mover (Role Changes)

Owner: @Owner
Evidence: Access change records

- Role changes trigger access re-evaluation
- Old access removed promptly
- Access changes require approval
- No informal role-based access changes

Notes / Exceptions:

- ...

3.3 Leaver (Offboarding)

Owner: @Owner
Evidence: Offboarding logs / deprovisioning reports

- Access revoked on termination date
- SaaS, cloud, and on-prem systems covered
- Service accounts reviewed upon departure
- Offboarding evidence retained

Notes / Exceptions:

- ...

4. Privileged Access Governance

SOC 2 CC Mapping:

- CC6.1 – Logical access restriction
- CC6.2 – Provisioning of privileged access
- CC6.3 – Modification and removal of access

Control Objective: Privileged access is minimal, justified, and monitored.
Control Owner: @Owner

Evidence: Admin access reports / PAM logs

- Privileged roles clearly defined
- Privileged access limited and justified
- Privileged access time-bound or periodically reviewed
- No default or standing admin access without approval
- Privileged access reviewed more frequently
- Break-glass access documented and logged
- Privileged actions logged

Notes / Exceptions:

- ...

5. User Access Reviews (UAR)

SOC 2 CC Mapping:

- CC6.3 – Periodic access reviews
- CC6.1 – Continued authorization validation

Control Objective: Access is reviewed regularly and decisively.
Control Owner: @Owner
Review Frequency: Quarterly / Monthly

Evidence: Access review reports

- Reviews conducted on defined cadence
- Critical systems included
- Reviews performed by responsible managers
- Explicit approve / revoke decisions captured
- Approval justifications recorded
- Revocations executed and verified
- Review completion tracked
- No spreadsheet- or email-based reviews

Last Review Completed: Date

Notes / Exceptions:

- ...

6. Segregation of Duties (SoD)

SOC 2 CC Mapping:

- CC6.3 – Logical access modification
- CC6.1 – Prevention of unauthorized access

Control Objective: Conflicting permissions are prevented or detected.
Control Owner: @Owner

Evidence: SoD policy / violation reports

- SoD requirements defined for sensitive workflows
- No user can both request and approve sensitive actions
- SoD evaluated across multiple systems
- Violations detected and resolved
- Exceptions documented with justification
- Continuous monitoring for new conflicts

Notes / Exceptions:

- ...

7. Service Accounts & Non-Human Identities

SOC 2 CC Mapping:

- CC6.1 – Logical access restriction
- CC6.2 – Non-human account provisioning
- CC6.3 – Non-human access modification

Control Objective: Non-human access is governed like human access.
Control Owner: @Owner

Evidence: Service account inventory

- All service accounts inventoried
- Each service account has a named owner
- Permissions follow least privilege
- Secrets / keys rotated regularly
- Unused service accounts removed
- Service account activity logged
- No personal accounts used for automation

Notes / Exceptions:

- ...

8. Orphaned, Dormant & Shadow Accounts

SOC 2 CC Mapping:

- CC6.1 – Logical access restriction
- CC6.2 – Timely deprovisioning

Control Objective: No access exists without accountability.
Control Owner: @Owner

Evidence: Dormant / orphaned account reports

- Dormant accounts identified regularly
- Dormant access revoked or re-approved
- Orphaned accounts eliminated
- Shadow IT applications discovered
- Access to unmanaged apps reviewed
- Identity sprawl continuously monitored

Notes / Exceptions:

- ...

9. Logging, Monitoring & Evidence Retention

SOC 2 CC Mapping:

- CC7.2 – Monitoring for anomalies
- CC7.3 – Event logging
- CC7.4 – Incident evidence retention

Control Objective: Identity activity is auditable and reproducible.
Control Owner: @Owner

Evidence: SIEM / audit logs

- Identity and access events logged
- Logs tamper-resistant
- Retention meets SOC requirements
- Evidence easily retrievable
- Audit trails show who approved what and when
- Evidence consistent across systems

Notes / Exceptions:

- ...

10. Risk-Based Identity Governance

SOC 2 CC Mapping:

- CC3.0 – Risk assessment
- CC6.1 – Risk-informed access control

Control Objective: Higher risk identities receive higher scrutiny.
Control Owner: @Owner

Evidence: Risk scoring reports

- High-risk identities identified
- Risk scores applied to users and permissions
- High-risk users reviewed more frequently
- Risk signals influence access decisions
- Risk posture documented and reviewed

Notes / Exceptions:

- ...

11. Policy Alignment & Reality Check

SOC 2 CC Mapping:

- CC2.1 – Policy establishment
- CC2.3 – Communication of policies
- CC6.1 – Enforcement of access policies

Control Objective: Policies reflect real-world behavior.
Control Owner: @Owner

Evidence: Policies + enforcement proof

- Access policies align with system behavior
- Identity governance explicitly covered
- Exceptions documented and approved
- Policy violations detected
- Violations remediated

Notes / Exceptions:

- ...

12. Audit Readiness & Ongoing Operations

SOC 2 CC Mapping:

- CC1.1 – Governance oversight
- CC1.2 – Accountability
- CC4.1 – Continuous improvement

Control Objective: SOC compliance is operational, not episodic.
Control Owner: @Owner

- Identity governance runs year-round
- Evidence generated continuously
- Audit prep does not rely on reconstruction
- Control owners understand responsibilities
- Identity governance metrics tracked
- SOC treated as an operating standard

Notes / Exceptions:

- ...

Final Internal Attestation

Prepared By: @Owner

Reviewed By: @Owner

Date: Date

Interested in learning more?
Schedule a demo.

Let us know where to reach you and a member of our team will contact you soon to schedule a time to walk through our solution!

Request a Demo