

SOC 2 Controls List

Controls	47
Category in scope	Security (the common criteria)
Criteria	Trust services criteria, 2017, with revised points of focus
Sized for	A small software company running production with one cloud provider

1. How to use this list

SOC 2 has no official list of controls. The AICPA publishes the trust services criteria, with points of focus that describe what each criterion can involve, and each company writes its own controls to meet them. An independent licensed CPA firm then tests the controls the company describes.

This list is one control set for a small software company with the Security category in scope: 47 controls, grouped below by the criterion series of the first criterion each one serves, with the policy that owns it and the evidence that shows it operates. The last section turns it around and lists, for every common criterion, the controls that map to it.

- Rewrite any control your company does not run exactly as written. The auditor tests what the description says.
- Name an owner for every control. The Excel version has an Owner column for it.
- Add a control for any criterion your company meets in a way this set does not describe.

2. CC1 Control environment

Code	Control	Criteria	Owning policy	Evidence that proves it
H3	Everyone completes security awareness training at hire and every year after.	CC1.4, CC2.2	Human Resources Security Policy	Screenshot of training completion report
B4	Every employee and contractor acknowledges the code of conduct.	CC1.1	Code of Conduct	Code of Conduct document or acknowledgment log
H1	Background checks are completed before a person starts.	CC1.4	Human Resources Security Policy	Redacted example of completed background check

Code	Control	Criteria	Owning policy	Evidence that proves it
H2	Every person signs a non-disclosure agreement at hire.	CC1.1, CC1.4	Human Resources Security Policy	NDA or confidentiality agreement template; Example of signed NDA (redacted)
R1	Management reviews the security and compliance program at least once a year.	CC1.2, CC4.1, CC5.3	Information Security Policy	Meeting notes or review documentation
B3	Security roles and responsibilities are documented and communicated.	CC1.3, CC2.2	Information Security Policy	RACI matrix or org chart showing security roles
B8	A body outside day to day management, such as a board or a named independent advisor, reviews security on a set schedule.	CC1.2, CC4.1	Information Security Policy	Minutes of the most recent review
B9	Security responsibilities are written into job descriptions or performance expectations for staff with production access.	CC1.5	Human Resources Security Policy	One job description or performance template showing those responsibilities (redacted)

3. CC2 Communication and information

Code	Control	Criteria	Owning policy	Evidence that proves it
Q2	Customers are told which controls they are responsible for (complementary user entity controls).	CC2.3	Third Party and Vendor Management Policy	Document showing customer responsibilities

4. CC3 Risk assessment

Code	Control	Criteria	Owning policy	Evidence that proves it
E1	A formal information security risk assessment is completed at least once a year.	CC3.1, CC3.2, CC3.3, CC3.4	Risk Management Policy	Risk assessment report or summary
E2	Identified risks and their mitigation actions are tracked in a risk register.	CC3.2	Risk Management Policy	Current risk register

Code	Control	Criteria	Owning policy	Evidence that proves it
E4	The risk assessment explicitly considers fraud and insider misuse.	CC3.3	Risk Management Policy	Risk assessment pages or register rows covering fraud and insider misuse
E5	Significant changes, such as new systems, vendors or headcount changes, are assessed for risk before rollout.	CC3.4, CC5.1	Risk Management Policy	One change where the risk assessment is visible before the rollout

5. CC4 Monitoring activities

Code	Control	Criteria	Owning policy	Evidence that proves it
K1	Logs from the application and the infrastructure are collected in one central place.	CC4.1, CC4.2, CC7.2	Operations Security Policy	Screenshot of log dashboard showing coverage
R2	Remediation items from audits, incidents, tests and reviews are tracked until they are closed.	CC4.2, CC5.3	Risk Management Policy	Screenshot of remediation tracker
R4	Control deficiencies are reported to management through a defined route, to named people.	CC4.2, CC2.1	Information Security Policy	One deficiency report or tracker entry that reached management (redacted)

6. CC6 Logical and physical access controls

Code	Control	Criteria	Owning policy	Evidence that proves it
G1	Multi-factor authentication is enforced for every sign-in to the cloud provider console.	CC6.1, CC6.6	Access Control Policy	Screenshot of MFA policy settings showing enforcement
G4	Access to production systems is granted through roles, each limited to what the job needs.	CC6.1, CC6.2, CC6.3	Access Control Policy	Screenshot or export of IAM roles/groups
I2	Every external connection to the service is encrypted with TLS.	CC6.7	Cryptography Policy	SSL Labs scan or TLS configuration screenshot
I3	Databases and backups are encrypted at rest.	CC6.1	Cryptography Policy	Screenshot of database/storage encryption settings

Code	Control	Criteria	Owning policy	Evidence that proves it
I1	Data is classified under a written scheme, and handling rules follow the classification.	CC6.1	Data Management Policy	Data Classification Policy or matrix
L1	A web application firewall or equivalent filters traffic to the service.	CC6.6	Operations Security Policy	Screenshot of WAF configuration/rules
F4	Every company laptop runs endpoint protection that is kept up to date.	CC6.8	Asset Management Policy	Screenshot showing endpoint protection coverage
G7	Access is removed within 24 hours of a termination.	CC6.2, CC6.3	Access Control Policy	Evidence of a recent termination access removal (redacted)
G8	All user access to production is reviewed on a documented schedule.	CC6.2, CC6.3, CC1.5	Access Control Policy	Most recent completed access review
G9	A named manager approves production access before it is granted.	CC6.2, CC6.3	Access Control Policy	One approved production access request with the approval visible (redacted)
H4	A documented offboarding checklist records access revocation for each departure.	CC6.2, CC1.4	Human Resources Security Policy	One completed offboarding record (redacted)
I10	Customer data has a set retention period and is securely disposed of at end of life.	CC6.5	Data Management Policy	Retention schedule or one deletion record (redacted)
F6	An inventory lists every production system, data store and SaaS application, each with an owner.	CC6.1, CC5.2, CC9.2	Asset Management Policy	Inventory showing each production system, data store and SaaS application with its owner

7. CC7 System operations

Code	Control	Criteria	Owning policy	Evidence that proves it
M1	Internal vulnerability scans run every month.	CC7.1	Operations Security Policy	Recent vulnerability scan report

Code	Control	Criteria	Owning policy	Evidence that proves it
O1	A written incident response plan exists and is approved by management.	CC7.3, CC7.4, CC7.5	Incident Response Plan	Incident Response Plan document
P1	Production databases and volumes are backed up on a set schedule.	CC7.5, CC9.1 (A1.2 when Availability is in scope)	Business Continuity and Disaster Recovery Plan	Screenshot of backup configuration
M3	A penetration test is performed every year.	CC7.1, CC4.1	Operations Security Policy	Penetration test report or its executive summary
M4	Critical patches are applied within 30 days.	CC7.1	Operations Security Policy	Patching policy or evidence of recent patching
O3	A root cause analysis is performed for every high severity incident.	CC7.4, CC7.5	Incident Response Plan	Root cause analysis for a recent high-severity incident (redacted)
P5	The disaster recovery and business continuity plan is tested at least once a year.	CC7.5, CC9.1 (A1.3 when Availability is in scope)	Business Continuity and Disaster Recovery Plan	DR test results or summary
K3	Alerts are configured for security events.	CC7.2, CC7.3	Information Security Policy	Screenshot of alert rules or recent alerts
M5	Production systems are configured to a documented hardening baseline.	CC7.1, CC5.2	Operations Security Policy	Baseline document or a configuration scan showing it applied

8. CC8 Change management

Code	Control	Criteria	Owning policy	Evidence that proves it
N1	Every change to production is tracked in a ticket or pull request.	CC8.1	Secure Development Policy	Screenshot of change tracking system; Example of a recent change (PR, ticket)
N2	Code is peer reviewed before it is deployed.	CC8.1	Secure Development Policy	Screenshot of branch protection settings; Example PR showing code review approval

Code	Control	Criteria	Owning policy	Evidence that proves it
N3	Development, test and production environments are separated.	CC8.1	Secure Development Policy	Diagram or screenshot showing environment separation
N4	Emergency changes follow a documented procedure.	CC8.1	Secure Development Policy	Emergency change procedure document; Example of a past emergency change
N5	Production deployments are approved by someone other than the author.	CC8.1	Secure Development Policy	One production release showing the recorded approval

9. CC9 Risk mitigation

Code	Control	Criteria	Owning policy	Evidence that proves it
Q1	Vendors are reviewed for security risk before onboarding and every year after.	CC9.2	Third Party and Vendor Management Policy	Vendor risk assessment template or completed assessment
C3	Each subservice organization provides a SOC report or completes a security questionnaire.	CC9.2	Third Party and Vendor Management Policy	One SOC report cover page or one completed security questionnaire (redacted)
Q3	A vendor register lists each vendor with production data access, its criticality and the date of its last review.	CC9.2	Third Party and Vendor Management Policy	Vendor register
C4	The SOC 2 report or security attestation of each subservice organization is reviewed every year.	CC9.2, CC4.1	Third Party and Vendor Management Policy	One completed review showing the report reviewed and the date

10. Controls by criterion

Every common criterion, and the two Availability criteria the set reaches when that category is in scope, with the controls that map to it.

Criterion	What it covers	Controls
CC1.1	Integrity and ethics	B4, H2

Criterion	What it covers	Controls
CC1.2	Board oversight	R1, B8
CC1.3	Structure and reporting	B3
CC1.4	Hiring and competence	H3, H1, H2, H4
CC1.5	Accountability	G8, B9
CC2.1	Reliable information	R4
CC2.2	Internal communication	H3, B3
CC2.3	External communication	Q2
CC3.1	Risk objectives	E1
CC3.2	Risk identification	E1, E2
CC3.3	Fraud risk	E1, E4
CC3.4	Changes that add risk	E1, E5
CC4.1	Control monitoring	K1, M3, R1, B8, C4
CC4.2	Fixing deficiencies	K1, R2, R4
CC5.1	Choosing controls	E5
CC5.2	Technology controls	F6, M5
CC5.3	Policies and procedures	R1, R2
CC6.1	Logical access	G1, G4, I3, I1, F6
CC6.2	User provisioning	G4, G7, G8, G9, H4
CC6.3	Least privilege	G4, G7, G8, G9
CC6.4	Physical access	None in this set. See How to use.
CC6.5	Data and device disposal	I10
CC6.6	Network boundaries	G1, L1
CC6.7	Data in transit	I2
CC6.8	Malware prevention	F4
CC7.1	Vulnerability monitoring	M1, M3, M4, M5

Criterion	What it covers	Controls
CC7.2	Anomaly monitoring	K1, K3
CC7.3	Incident triage	O1, K3
CC7.4	Incident response	O1, O3
CC7.5	Incident recovery	O1, P1, O3, P5
CC8.1	Change management	N1, N2, N3, N4, N5
CC9.1	Disruption risk	P1, P5
CC9.2	Vendor risk	Q1, C3, F6, Q3, C4
A1.2	Recovery infrastructure	P1
A1.3	Recovery testing	P5

CC6.4 covers physical access to facilities and equipment. A company with no data center of its own usually relies on its cloud provider for it, carved out of the report as a subservice organization, and controls C3 and C4 cover reviewing that provider's report. Add a physical access control if you keep servers or customer data in an office.

Source

Source: free template from www.polaralabs.com/templates/soc-2-controls-list (CC BY 4.0).