SURECLOUD®

EXECUTABLE GRC

SOC 2 Compliance Checklist.

Eight phases. One owner for every task. Evidence for every claim.

- Scope
- Type 1 or Type 2
- Control mapping
- Evidence
- Fieldwork
- Ongoing monitoring

Every control has to pass three tests before it counts: **documented, implemented, effective.**

BEFORE YOU START

Who owns it, and what proves it.

Most checklists tell you what to do. They don't tell you who owns it, or what proves it's done. This one does. Work through each phase in order, name an owner for every item, and file the evidence as you go, not the week before fieldwork.

Every control has to pass three tests

Documented

The control exists in a signed, dated, version-controlled policy that names its owner.

Implemented

The control is live in the systems in scope, not just described on paper.

Effective

It operated consistently across the whole observation period, with evidence to show it.

The eight phases

PHASE	WHAT IT COVERS	OWNER
1	**Define your scope**	Compliance lead / CISO
2	**Choose Type 1 or Type 2**	Compliance lead / CISO
3	**Map controls to Trust Services Criteria**	Compliance lead / security team
4	**Create and approve policies**	Compliance lead / legal
5	**Collect audit evidence**	Control owners
6	**Remediate gaps before fieldwork**	Compliance lead
7	**Prepare for audit**	Compliance lead
8	**Maintain compliance after audit**	Compliance lead

1 PHASE ONE

Define your scope.

Scope sets the boundary of the report: the systems, the services, the people, and the Trust Services Criteria you'll be assessed against. Get it signed off before anything else starts.

Systems and people in scope

- [ ] List every system that touches customer data (production databases, CI/CD pipelines, etc.)
- [ ] Name every customer-facing service that's in scope
- [ ] Identify every team and role with access to in-scope systems
- [ ] Inventory third-party vendors that process or store data, including cloud providers

Trust Services Criteria to include

- [ ] Confirm Security (Common Criteria, CC1 to CC9): mandatory for every report MANDATORY
- [ ] Decide if Availability applies: check contracts for uptime SLAs
- [ ] Decide if Confidentiality applies: sensitive business data beyond PII
- [ ] Decide if Processing Integrity applies: customers rely on accurate transaction processing
- [ ] Decide if Privacy applies: you collect or disclose personal data
- [ ] Get the finalised scope signed off

OWNER	EVIDENCE
Compliance lead / CISO	**Scope document, system inventory**

2 PHASE TWO

Choose Type 1 or Type 2.

The type you choose sets the shape of everything downstream: how long you collect evidence for, how the auditor tests, and when you can hand a report to a customer.

- [ ] Decide between a point-in-time report (Type 1) or an observation-period report (Type 2)
- [ ] Confirm the observation period if Type 2 (typically 6 to 12 months)
- [ ] Check enterprise customer contracts for a Type 2 requirement
- [ ] Set your audit timeline around the type you choose

OWNER	EVIDENCE
Compliance lead / CISO	**Audit type decision, timeline**

Type 1 and Type 2 at a glance

DIMENSION	TYPE 1	TYPE 2
What it reports	Control design at a single point in time	Control design and operating effectiveness over a period
Observation period	None — as at a specified date	Typically 6 to 12 months
Auditor testing	Design of controls only	Sampling across the observation period
Best for	A first report, or proving design ahead of a Type 2	Enterprise contracts that specify Type 2

3

PHASE THREE

Map controls to Trust Services Criteria.

Every criterion in scope needs at least one control mapped to it, and every control needs to clear all three tests: documented, implemented, effective.

- [ ] Map access controls: provisioning, role-based access, MFA, access reviews
- [ ] Map change management: code review, deployment approvals, rollback
- [ ] Map incident response: detection, classification, escalation, post-incident review
- [ ] Map risk assessment: formal risk register, annual review
- [ ] Map vendor management: inventory, due diligence, sub-processor register
- [ ] Map security monitoring: log aggregation, alert thresholds, penetration testing
- [ ] Confirm every control is documented in policy
- [ ] Confirm every control is actually implemented
- [ ] Confirm every control operated effectively across the observation period

OWNER	EVIDENCE
Compliance lead / security team	**Control matrix**

4

PHASE FOUR

Create and approve policies.

Five policies carry most of the weight. Each one needs a named owner, a signature, a date, a version number, and a review cycle. An unsigned policy is not a control.

Draft the five core policies

- [ ] Draft information security policy: objectives, responsibilities, governance
- [ ] Draft access control policy: provisioning, reviews, revocation, MFA
- [ ] Draft vendor risk policy: assessment, onboarding, monitoring, offboarding
- [ ] Draft incident response policy: detection through to review
- [ ] Draft business continuity policy: RTOs, backup, disaster recovery testing cadence

Approve, publish, and diarise

- [ ] Get every policy signed off by its named owner (CISO or equivalent)
- [ ] Date and version-control every policy
- [ ] Communicate policies to staff and keep evidence of that communication
- [ ] Schedule an annual review date for every policy

OWNER	EVIDENCE
Compliance lead / legal	**Signed, dated policy documents**

5

PHASE FIVE

Collect audit evidence.

Evidence is what turns a described control into a tested one. Collect it as the control operates, timestamped and attributable, and file it against the control it proves.

- [ ] Capture timestamped screenshots from your identity provider and cloud console
- [ ] Pull system-generated logs showing expected security events
- [ ] Complete access reviews (quarterly or semi-annual) and file the records
- [ ] Close change tickets with a visible approval workflow
- [ ] File signed, dated policy documents
- [ ] Collect vendor SOC 2 reports or security questionnaires
- [ ] Store everything in one evidence repository, organised by control

OWNER	EVIDENCE
Control owners	**Evidence repository**

Where teams lose the most time: manual evidence collection. Automating it against your control framework cuts that effort by 50 to 65%.

6

PHASE SIX

Remediate gaps before fieldwork.

Work the list in this order:

- [ ] **First:** controls with no evidence at all
- [ ] **Second:** controls that are designed but not implemented
- [ ] **Third:** controls that are implemented but inconsistently evidenced
- [ ] Assign a named owner to every gap
- [ ] Log exceptions formally with rationale and a resolution date
- [ ] Document remediation with evidence: ticket, config change, or policy update

OWNER	EVIDENCE
Compliance lead	**Remediation log, exception register**

7

PHASE SEVEN

Prepare for audit.

Fieldwork goes fastest when the auditor never has to ask twice. Organise the pack, name the people, and agree the schedule before the first interview.

- [ ] Organise evidence by control and Trust Services Criteria category, with dates and sources
- [ ] Name a contact for every control area
- [ ] Agree the fieldwork schedule with your auditor in advance
- [ ] Brief every control owner before their interview
- [ ] Assign one point of contact for all auditor information requests
- [ ] Prepare for sampling across the observation period (Type 2)
- [ ] Prepare system exports for control testing
- [ ] Build in time to handle follow-up information requests

OWNER	EVIDENCE
Compliance lead	**Evidence pack, walkthrough notes**

8

PHASE EIGHT

Maintain compliance after audit.

The report is a snapshot; the controls keep running. Monitoring, reminders, and re-used evidence are what stop the next cycle starting from zero.

- [ ] Set up continuous monitoring: automated alerts for drift, anomalies, violations
- [ ] Automate reminders for access reviews, policy reviews, vendor assessments
- [ ] Re-use evidence across other frameworks you hold (ISO 27001, NIST CSF)
- [ ] Map new requirements to existing controls as frameworks evolve
- [ ] Calendar the next audit cycle before this one closes

OWNER	EVIDENCE
Compliance lead	**Monitoring reports, updated evidence**

The thread through all eight phases.

Named ownership. Every task on this list fails without someone accountable for it, and every control fails without evidence that's documented, implemented, and effective. Print this, assign it, and work it phase by phase.

POWERED BY GRACIE

READY TO STOP CHASING SCREENSHOTS?

Spend less time proving controls, more time fixing the gaps that matter.

Gracie AI Agents with Personas and Skills cut manual evidence collection by 50 to 65%, so your team spends less time proving controls and more time fixing the gaps that matter.

50–65%	8	1
Less time spent on manual evidence collection	Phases tracked against a single control framework	Named owner and evidence trail per control

GUIDE	**SOC 2 Readiness Guide**	surecloud.com/resource-hub
DEEP DIVE	**Trust Services Criteria Explained**	surecloud.com/resource-hub
TEMPLATE	**Control Matrix and Evidence Register**	surecloud.com/resource-hub
RELATED	**ISO 27001 ISMS Design Workbook**	surecloud.com/resource-hub

See SureCloud in action.

Gracie AI Agents and Skills automate the evidence collection, monitoring, and audit-trail work your SOC 2 report demands — at scale.

Book your demo →