SOC 2 · CONTINUOUS COMPLIANCE · 46-POINT FIELD CHECKLIST

The SOC 2 Continuous Compliance Checklist.

46 controls mapped to CC1–CC9 plus the continuous-evidence layer that legacy GRC platforms (Vanta, Drata, Secureframe) leave out.

PUBLISHED BY
Ogynx · Veritra

FRAMEWORK
AICPA SOC 2 TSC 2017

USE WITH
ISO 27001 · HIPAA · PCI

ogynx.com/resources

HOW TO USE THIS CHECKLIST

From spreadsheet to continuous evidence in six weeks.

This is the checklist we use inside Veritra to move teams from an ad-hoc SOC 2 posture to **continuous, evidence-fresh readiness**. Every control is mapped to the AICPA Trust Services Criteria (CC1–CC9), scored on a 0–3 maturity scale, and tagged with the collector or automation that keeps it green between audits.

SCORE	STATE	WHAT IT MEANS
0	Missing	No control, no owner, no evidence.
1	Ad-hoc	Someone does it, occasionally. Not documented.
2	Documented	Policy + owner exist. Evidence collected manually.
3	Continuous	Automated collector; evidence refreshed on a schedule.

THE SIX-WEEK PATH

WEEK 1	**Baseline**	Score every control 0–3. Identify owners. Nothing else.
WEEK 2	**Close the 0s**	Draft policies, assign owners, stand up the missing controls.
WEEK 3–4	**Automate the 1s and 2s**	Wire collectors (cloud, IdP, HRIS, code) so evidence refreshes without humans.
WEEK 5	**Dry-run**	Give an auditor read-only access. Fix whatever they can't find in <30 seconds.
WEEK 6	**Type I**	Point-in-time report. Type II observation window starts the next day.

CC1 Control Environment

Governance, tone, and organizational integrity.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Documented code of conduct signed by every employee at hire.	HRIS attestation	Annual	0 1 2 3
2	Board or executive sponsor named for the security program.	Charter document	Annual	0 1 2 3
3	Org chart with defined security roles (CISO, DPO, incident lead).	HRIS export	Quarterly	0 1 2 3
4	Background checks completed before production access is granted.	HRIS + provisioning log	Per hire	0 1 2 3
5	Annual performance review includes security responsibilities.	HRIS review record	Annual	0 1 2 3

CC2 Communication & Information

How the org shares security-relevant information.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Security policies published in a location every employee can reach.	Intranet / handbook link	On update	0 1 2 3
2	Whistleblower / anonymous reporting channel exists and is tested.	Ticket audit	Quarterly	0 1 2 3
3	Customer-facing security page (trust center) with current status.	Public URL	Continuous	0 1 2 3
4	Incident-communication plan names the customer-comms owner.	Runbook	Annual	0 1 2 3

CC3 Risk Assessment

Identifying and evaluating risks to objectives.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Risk register with owner, likelihood, impact, treatment for every entry.	Register export	Quarterly	0 1 2 3
2	Fraud risks explicitly considered (financial, insider, AI-generated).	Risk register tag	Annual	0 1 2 3
3	Threat model refreshed after every material architecture change.	Threat-model doc	Per change	0 1 2 3
4	Vendor risk assessment for every subprocessor handling customer data.	Vendor register	Annual + on add	0 1 2 3
5	AI / model risk register if you ship or use LLMs.	AI inventory	Quarterly	0 1 2 3

CC4 Monitoring Activities

Ongoing evaluation of controls.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Internal control testing schedule with named tester per control.	Test log	Quarterly	0 1 2 3
2	Deficiencies tracked in a ticket system with due date and owner.	Ticket export	Continuous	0 1 2 3
3	Management reviews control results at least quarterly.	Meeting minutes	Quarterly	0 1 2 3
4	Continuous monitoring platform in place (not just annual sweep).	Platform screenshot	Continuous	0 1 2 3

CC5 Control Activities

The controls themselves — technical and procedural.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Separation of duties enforced for production deploys and financial actions.	IAM policy	Continuous	0 1 2 3
2	Change-approval workflow required before any prod merge.	Git branch protection	Continuous	0 1 2 3
3	Automated tests block deploy on failed security checks.	CI config	Continuous	0 1 2 3

CC6 Logical & Physical Access

Access controls — the highest-scrutiny area for auditors.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	SSO enforced for every SaaS app that supports it.	IdP app inventory	Continuous	0 1 2 3
2	MFA required for every human account, no exceptions.	IdP MFA report	Continuous	0 1 2 3
3	Least-privilege reviewed quarterly; unused accounts disabled in 24h.	Access review export	Quarterly	0 1 2 3
4	Offboarding revokes all access within 24 hours of termination.	HRIS > IdP diff	Per event	0 1 2 3
5	Production database access is time-bound and logged.	Break-glass log	Continuous	0 1 2 3
6	Encryption at rest for all customer data (AES-256 or equivalent).	Cloud config export	Continuous	0 1 2 3
7	Encryption in transit (TLS 1.2+) enforced on every public endpoint.	TLS scan	Weekly	0 1 2 3
8	Endpoint MDM enforces disk encryption, screen lock, patch level.	MDM compliance	Continuous	0 1 2 3
9	Physical access to any on-prem hardware logged and reviewed.	Badge log	Monthly	0 1 2 3

CC7 System Operations

Detecting and responding to what goes wrong in production.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Vulnerability scan of production infra at least weekly.	Scanner report	Weekly	0 1 2 3
2	Penetration test with reproducible evidence at least annually.	Pentest report + PoC	Annual +	0 1 2 3
3	SIEM or equivalent log aggregation for all production systems.	SIEM dashboard	Continuous	0 1 2 3
4	Anomaly alerts routed to on-call with defined SLA.	PagerDuty policy	Continuous	0 1 2 3
5	Incident response plan tested with a tabletop exercise annually.	Tabletop notes	Annual	0 1 2 3
6	Post-incident review within 5 business days of every Sev-1/2.	Post-mortem doc	Per incident	0 1 2 3

CC8 Change Management

How code and infra changes reach production.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	All infra managed as code and version-controlled.	IaC repo	Continuous	0 1 2 3
2	Pull-request review required from a second engineer.	Git branch protection	Continuous	0 1 2 3
3	Rollback tested and documented for every production service.	Runbook + drill log	Quarterly	0 1 2 3

CC9 Risk Mitigation

Insurance, BC/DR, and vendor risk.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Business continuity plan with named owner and RTO/RPO targets.	BCP doc	Annual	0 1 2 3
2	Disaster recovery restore tested end-to-end at least annually.	DR test report	Annual	0 1 2 3
3	Cyber insurance policy in force with coverage limits reviewed.	Policy binder	Annual	0 1 2 3
4	Subprocessor list published and updated on customer-facing page.	Public URL	Continuous	0 1 2 3

EV Continuous Evidence Layer

The gap legacy GRC leaves — automate this or the checklist decays.

#	CONTROL	EVIDENCE	FREQUENCY	MATURITY
1	Every control has an automated collector — no human screenshots.	Collector inventory	Continuous	0 1 2 3
2	Evidence freshness dashboard visible to the security team.	Platform metric	Continuous	0 1 2 3
3	Auditor has read-only access to the live control state.	Auditor account	Continuous	0 1 2 3
4	Drift alerts fire within 15 minutes of a failing control.	Alert log	Continuous	0 1 2 3
5	Pentest findings pipe directly into CC7.1 / CC8.1 evidence.	Integration config	Continuous	0 1 2 3

APPENDIX · FRAMEWORK CROSSWALK

One collector, many frameworks.

Every control in this checklist maps to more than SOC 2. Wire the collector once and the evidence satisfies your ISO 27001, HIPAA, and PCI obligations at the same time.

OGYNX CONTROL AREA	SOC 2 TSC	ISO 27001:2022	HIPAA	PCI DSS 4.0
Access management	CC6.1–6.3	A.5.15, A.5.18, A.8.2	§164.308(a)(4)	Req. 7, 8
Encryption	CC6.7	A.8.24	§164.312(a)(2)(iv)	Req. 3, 4
Vulnerability + pentest	CC7.1, CC8.1	A.8.8, A.8.29	§164.308(a)(1)(ii)(A)	Req. 6, 11.3, 11.4
Change management	CC8.1	A.8.32	§164.308(a)(5)(ii)(D)	Req. 6.5
Incident response	CC7.3–7.5	A.5.24–A.5.28	§164.308(a)(6)	Req. 12.10
Vendor risk	CC9.2	A.5.19–A.5.22	§164.308(b)	Req. 12.8
BC / DR	CC9.1, A1.2	A.5.29–A.5.30	§164.308(a)(7)	Req. 12.10.1
Risk assessment	CC3.1–3.4	Clause 6.1, A.5.4	§164.308(a)(1)(ii)(A)	Req. 12.3
Monitoring / logging	CC7.2	A.8.15–A.8.17	§164.312(b)	Req. 10

AUDIT-DAY READINESS · THE 30-SECOND TEST

For every control on this checklist, an auditor should be able to answer three questions in under 30 seconds without pinging your team. If they can't, the control is not continuous.

Who owns it?	A named person, not a team, not a Slack channel.
Where's the evidence?	A live dashboard or query — not a shared drive of screenshots.
When was it last verified?	A timestamp from the collector, refreshed within the last cycle.

SIGN-OFF

Program owner	______________________	**Date**	______________
Reviewed by	______________________	**Date**	______________

Auditor of record		**Date**	

AUTOMATE THIS CHECKLIST

Veritra runs it for you — continuously.

Every control above becomes an automated collector. Evidence refreshes on a schedule. Drift alerts fire in minutes. Your auditor logs in and reviews live state.

veritra.ogynx.com