CHECKLIST · SOC 2

SOC 2 Audit Readiness Checklist (CC Series)

Step-by-step checklist for Common Criteria controls — check your readiness before engaging an auditor.

3 pages · PDF · Updated May 2026 · **goironfort.com**

This checklist covers the AICPA Trust Service Criteria Common Criteria (CC) series — the mandatory security category required for every SOC 2 examination. Complete this before engaging an auditor to avoid costly remediation during fieldwork.

CC1 — Control Environment

- ☐ Board or management has approved an information security policy
- ☐ Security roles and responsibilities are formally defined
- ☐ Security awareness training completed by all workforce members in last 12 months
- ☐ Background checks completed for all personnel with ePHI/customer data access

CC2 — Communication & Information

- ☐ Internal communication channels for security incidents are defined
- ☐ Security responsibilities communicated to external parties (vendors, customers)
- ☐ System description / management assertion prepared and reviewed by legal

CC3 — Risk Assessment

- ☐ Annual risk assessment completed and documented
- ☐ Risk register maintained and reviewed by management
- ☐ New risks identified from infrastructure changes are assessed before deployment

CC4 — Monitoring Activities

- ☐ Continuous monitoring tools deployed across in-scope infrastructure

© 2026 Iron Fort Solutions Inc. | goironfort.com

Not legal advice · For informational purposes only

- Security metrics reported to management on a defined schedule
- Internal audit or self-assessment completed in the past 12 months

CC5 — Control Activities

- Change management policy in place with formal approval workflows
- Separation of duties enforced for production deployments
- Documented secure coding / development standards in use

CC6 — Logical & Physical Access

- MFA enabled for all user access to in-scope systems
- Access reviews conducted and documented quarterly
- Terminated employee access revoked within 24 hours
- Encryption at rest and in transit for customer data
- Intrusion detection / prevention systems deployed

CC7 — System Operations

- Vulnerability scanning program active (at least monthly)
- Incident response plan documented, tested, and current
- Security incident log maintained for last 12 months
- Backup and recovery procedures tested and documented

CC8 — Change Management

- All code changes go through a reviewed and approved change control process
- Pre-production testing environment separate from production
- Rollback procedures documented and tested

CC9 — Risk Mitigation

- Business continuity plan documented and tested
- Vendor risk management program active — all in-scope vendors assessed
- SOC 2 reports (or equivalent) collected from critical vendors
- Vendor agreements include security and data protection requirements

© 2026 Iron Fort Solutions Inc. | goironfort.com

Not legal advice · For informational purposes only

■ *Iron Fort continuously monitors all CC-series controls and auto-collects evidence for your auditor. Book a free scoping call at goironfort.com/demo*

© 2026 Iron Fort Solutions Inc. | goironfort.com

Not legal advice · For informational purposes only