SOC 2 Readiness Checklist

30 pre-audit readiness activities across the five AICPA Trust Services categories, for Australian SaaS teams.

Mindset Cyber
mindsetcyber.com.au

SOC 2 is an attestation performed by a licensed CPA firm against the AICPA Trust Services Criteria. The Security category (the Common Criteria) applies to every SOC 2; you add Availability, Processing Integrity, Confidentiality and/or Privacy based on the commitments you make to customers. Use this checklist to prepare the controls and evidence before you engage an auditor. Type 1 assesses design at a point in time; Type 2 assesses operating effectiveness over a period (commonly 3 to 12 months).

Security (Common Criteria) Required for every SOC 2.

- [ ] **Assign management oversight of security and document your information security policy set (approved and communicated).**
  Evidence: Org chart, security policy set, approval and communication records
- [ ] **Run a documented risk assessment at least annually; identify, rate, and treat risks.**
  Evidence: Risk assessment methodology, risk register with treatments
- [ ] **Enforce logical access controls: unique IDs, least privilege, role-based access, and MFA on key systems.**
  Evidence: Access control policy, MFA configuration, role definitions
- [ ] **Provision and de-provision access for joiners, movers, and leavers on time; review access periodically.**
  Evidence: Onboarding/offboarding tickets, periodic access review records
- [ ] **Follow a change management process with testing and approval before production changes.**
  Evidence: Change tickets, approvals, code review / CI records
- [ ] **Assess and monitor third-party vendors; include security terms in contracts.**
  Evidence: Vendor inventory, due-diligence records, signed DPAs
- [ ] **Run vulnerability scanning and patching on a defined cadence; obtain a penetration test.**
  Evidence: Scan reports, patch records, penetration test report and remediation
- [ ] **Log, alert on, and review security events; keep time-synced logs for a defined retention period.**
  Evidence: Logging / SIEM configuration, alert and review records
- [ ] **Maintain and test an incident response plan; log and review incidents.**
  Evidence: Incident response plan, exercise records, incident log
- [ ] **Deliver security awareness training at hire and at least annually.**
  Evidence: Training content and completion records
- [ ] **Cover physical and environmental controls (often inherited from your cloud provider).**
  Evidence: Cloud provider SOC reports, facility access records where applicable

Availability Optional: include if you commit to uptime or availability.

- [ ] **Define availability commitments (SLAs) and monitor capacity and performance against them.**
  Evidence: SLA definitions, monitoring dashboards, uptime reports
- [ ] **Back up critical data and test restoration.**
  Evidence: Backup configuration, restore test records
- [ ] **Document and test a disaster recovery / business continuity plan with defined RTO and RPO.**
  Evidence: DR/BCP plan, DR test results, RTO/RPO targets
- [ ] **Design redundancy or failover for critical components.**
  Evidence: Architecture diagram, failover test records

Processing Integrity Optional: include if you commit to complete, accurate, timely processing.

- [ ] **Validate inputs and handle errors so processing is complete, accurate, and authorised.**
  Evidence: Validation rules, error-handling design and logs
- [ ] **Monitor processing (jobs, queues) and reconcile outputs.**
  Evidence: Processing monitoring, reconciliation records
- [ ] **Apply data quality checks and review outputs.**
  Evidence: QA and reconciliation records
- [ ] **Apply change controls to processing logic specifically.**
  Evidence: Change tickets for processing components

Confidentiality Optional: include if you commit to protecting confidential information.

- [ ] **Classify data and identify what is confidential.**
  Evidence: Data classification policy, data inventory
- [ ] **Encrypt confidential data in transit and at rest.**
  Evidence: TLS configuration, at-rest encryption settings
- [ ] **Restrict access to confidential data on a need-to-know basis.**
  Evidence: Access controls, access review records
- [ ] **Define retention and secure disposal for confidential data.**
  Evidence: Retention schedule, secure disposal records
- [ ] **Put confidentiality agreements in place with staff and vendors.**
  Evidence: Signed NDAs and DPAs

Privacy Optional: include if you handle personal information.

- [ ] **Publish a privacy notice covering collection, use, retention, and disclosure.**
  Evidence: Published privacy policy / notice
- [ ] **Provide consent and choice mechanisms where required.**
  Evidence: Consent records, preference management
- [ ] **Operate a data subject request process (access, correction, deletion).**
  Evidence: DSAR procedure and request log
- [ ] **Limit collection to stated purposes and enforce retention limits.**
  Evidence: Data map, retention schedule
- [ ] **Put processor agreements in place for personal data shared with third parties.**
  Evidence: Signed DPAs
- [ ] **Dispose of personal information per your retention policy.**
  Evidence: Disposal records

Train the person who owns SOC 2: **PECB Lead SOC 2 Analyst course**.
