# SOC 2 Readiness Checklist

A practical starting point for SaaS and commercial teams preparing to organize their security controls and evidence.

**How to use this checklist:** Mark each item as Not Started, In Progress, Implemented, or Not Applicable. Assign an owner and keep evidence links in a controlled location. Applicability depends on your service, scope, and selected Trust Services Criteria.

## Scope & ownership

- ■ Define the service, product, and system boundary in scope.
- ■ Identify relevant infrastructure, cloud services, repositories, and production environments.
- ■ Map sensitive data types, data flows, storage locations, and integrations.
- ■ Identify key vendors and subservice organizations.
- ■ Assign control owners and an executive sponsor.

## Policies & risk management

- ■ Document security responsibilities and approval processes.
- ■ Maintain a risk register with owners, treatment decisions, and review dates.
- ■ Review and approve security policies; track staff acknowledgement where appropriate.
- ■ Define a process for security exceptions and risk acceptance.
- ■ Establish a recurring cadence for policy and risk reviews.

## Identity & access management

- ■ Require unique user accounts and appropriate authentication controls.
- ■ Use multi-factor authentication where appropriate, especially for privileged access.
- ■ Limit access using least privilege and role-based permissions.
- ■ Review access periodically and remove access promptly when no longer needed.
- ■ Protect and review privileged, service, and emergency accounts.

## Change & system operations

- ■ Document the process for proposing, reviewing, testing, and approving changes.
- ■ Separate development, test, and production access where practical.
- ■ Maintain code review and deployment records for relevant changes.
- ■ Define vulnerability identification, prioritization, and remediation processes.
- ■ Track backups, restoration testing, monitoring, and operational incidents.

## Incident response & continuity

- ■ Document how staff report suspected security incidents.
- ■ Define incident triage, escalation, investigation, and communication roles.
- ■ Maintain an incident response plan and test it periodically.
- ■ Define backup, recovery, and business continuity expectations.
- ■ Record lessons learned and follow-up actions after incidents or exercises.

## People, vendors & training

- ■ Provide security awareness training appropriate to staff roles.
- ■ Define onboarding, role changes, and offboarding security steps.
- ■ Inventory important vendors and assess security risks proportionately.
- ■ Document vendor review decisions, exceptions, and follow-up actions.
- ■ Set expectations for confidentiality and acceptable use.

## Evidence & monitoring

- ■ Create an evidence inventory mapped to controls and owners.
- ■ Keep dated records that show controls operate over time, not only policy documents.
- ■ Track control failures, exceptions, corrective actions, and completion evidence.
- ■ Define metrics or status reporting for key risks and remediation progress.
- ■ Confirm evidence access is limited and retention is appropriate.

## Suggested tracker columns

| Control / task | Status | Owner | Evidence / due date |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Important:** This checklist is educational and is not an official AICPA checklist, legal advice, or a guarantee of SOC 2 readiness or report issuance. A SOC 2 examination and report are performed by an independent licensed CPA firm. Tailor the work to your service, risks, scope, and applicable criteria.