

SOC 2 Readiness — Top 10 Controls

The highest-impact controls, pulled from our 85-point SOC 2 Readiness checklist.

Start here. These are the controls that block the most risk (and the ones auditors and cyber-insurance carriers ask about first). Work top-down — severity is highest at the top.

- CRITICAL** **Run a formal, documented risk assessment process.**
Verify: Adopt a written methodology for identifying, analyzing, and rating risks to your objectives.
- CRITICAL** **Require approval before any access is granted (formal access provisioning).**
Verify: Route all access requests through documented approval before provisioning.
- CRITICAL** **Enforce MFA for all remote access to production systems.**
Verify: Require a second factor for VPN, SSO, and any production login.
- CRITICAL** **Limit privileged/admin access to personnel with a clear business need.**
Verify: Restrict admin roles, justify each one, and prefer just-in-time elevation.
- CRITICAL** **Enable security event logging on all production systems.**
Verify: Turn on audit/security logging across servers, apps, and infrastructure.
- CRITICAL** **Put all production changes through a defined change management process.**
Verify: Require request, review, approval, and tracking for every production change.
- HIGH** **Maintain an organizational chart that shows clear lines of authority and responsibility.**
Verify: Publish a current org chart and role descriptions defining who reports to whom and who owns what.
- HIGH** **Assign security and compliance responsibilities to specific, named individuals.**
Verify: Name an accountable owner (e.g., CISO or security lead) and document each person's security duties.
- HIGH** **Document and version-control security policies and procedures.**
Verify: Store policies in a system that tracks changes, owners, and approval dates.
- HIGH** **Give every new hire security awareness training during onboarding.**
Verify: Require security training before or during the first week and track completion.

Want all 85 controls? The complete StronDEX SOC 2 Readiness pack includes every control with step-by-step verify/fix guidance, a branded PDF, and an interactive progress tracker.

Get it at stronDEX.com → Products