READINESS

SOC Readiness: Documentation & Evidence Checklist

A management checklist for organizing control documentation and evidence before examination fieldwork.

How to use this checklist

For each applicable area, identify the control owner, expected frequency, retained evidence, population source, and reviewer. Applicability depends on the report type and scope.

Area	Documentation to organize	Examples of evidence
Governance & risk	Governance structure; risk assessment; policies; oversight; control ownership.	Approvals; meeting minutes; risk register; policy reviews; follow-up tracking.
Logical access	Provisioning; modification; termination; privileged access; authentication; periodic review.	Tickets; approvals; access listings; review sign-offs; exception follow-up; configuration evidence.
Change management	Authorization; testing; segregation; migration; emergency changes.	Change tickets; approvals; test results; deployment logs; emergency-change review.
IT operations	Job monitoring; backups; restoration; vulnerability and patch management; capacity.	Monitoring logs; backup results; restore tests; scan reports; patch records; investigation evidence.
Incident response	Identification; escalation; containment; investigation; communication; lessons learned.	Incident records; severity decisions; communications; root-cause analysis; corrective actions.
Vendor oversight	Due diligence; contracts; risk tiering; monitoring; SOC report review; issue follow-up.	Assessments; contracts; vendor inventory; review documentation; CUEC mapping; remediation tracking.
Business continuity	Business impact; continuity plans; disaster recovery; testing; plan maintenance.	Approved plans; test scenarios; results; lessons learned; remediation; management approval.
Data protection	Classification; retention; encryption; transfer; disposal; confidentiality commitments.	Inventories; configurations; approvals; retention records; disposal evidence; monitoring.
Processing controls	Input, authorization, processing, reconciliation, output, and error handling.	Source records; reconciliations; exception reports; approvals; investigation and correction.
Privacy, if applicable	Notice; choice and consent; collection; use; retention; access; disclosure; monitoring.	Notices; inventories; requests; approvals; disclosures; complaint records; privacy assessments.

Evidence quality checks

- Evidence identifies the control, period, preparer or system source, reviewer, and date of performance.
- Screenshots include enough context to identify the system, population, settings, or record being reviewed.
- Review controls document the criteria used, items investigated, conclusions, and follow-up.
- Control populations can be generated completely and accurately and reconciled when appropriate.
- Evidence exists for the full Type 2 period and matches the stated control frequency.
- Exceptions are retained with investigation, resolution, approval, and remediation evidence.
- Policies describe actual practice and do not promise control activities the organization does not perform.

Readiness tracking fields

Field	What management should record
Control owner	Person accountable for performance and timely evidence retention.
Frequency	Event-driven, daily, weekly, monthly, quarterly, annual, or continuous.
Population source	System report, ticket queue, log, register, or other complete source.
Evidence location	Repository path and naming convention used for retained evidence.
Reviewer	Person who evaluates performance, exceptions, and follow-up.
Gap status	Issue, remediation owner, due date, implementation date, and validation evidence.

Readiness support and independence

A CPA firm may provide permitted readiness observations and recommendations, but management must make decisions, establish controls, assign competent owners, prepare the system description and assertion, and accept responsibility for remediation. Independence should be evaluated before work begins.

Important information

This resource is for general educational purposes and is not a substitute for professional advice or engagement-specific planning. Scope, criteria, controls, evidence, timing, and independence considerations vary. Management remains responsible for its system, controls, documentation, risk assessment, and assertions.