PANDORA CLOUD
UNPACKING COMPLEXITY

SOC 2 Readiness Checklist

Trust services criteria readiness for legal, insurance, and other regulated SMBs

A Pandora Cloud Buyer's Resource

May 2026

Pandora Cloud LLC
Women-Owned Small Business (WOSB) | AWS Advanced Partner
GSA MAS: 47QTCA24D00D3 | CAGE: 9JSG7 | UEI: R36GQ3N4XT63
Secret Facility Clearance | pandoracloud.net

About This Checklist

The Service Organization Control 2 (SOC 2) audit has become a non-negotiable contract gate for legal practices, insurance brokerages, claims operations, and other professional services firms selling into enterprise buyers, banks, hospital systems, and large carriers. Renewal cycles increasingly require a current Type II report. New deals stall when the security questionnaire arrives and there is nothing to attach.

This checklist is for the Small and Medium-sized Businesses (SMBs) preparing for their first SOC 2, dealing with a slipping renewal, or trying to determine whether the program they have today will hold up under a Type II audit window. It is structured around what auditors actually test in firms with fewer than 100 people, written for a managing partner or operations lead rather than a security engineer, and designed to surface gaps in an afternoon of work.

Use the 36-item checklist to score your current readiness. Use the 90-day path to plan your move from current state to audit kickoff. Use the audit-findings reference to know what you are most likely to be flagged on and how to fix it before the auditor arrives.

Reading time: 25 minutes if you are scoring yourself; 60 to 90 minutes if you are walking through it with the team.

Why SOC 2 Has Become a Contract Gate

Three shifts in the last twenty-four months explain why SOC 2 is showing up in so many SMB sales conversations.

1. Enterprise procurement teams have standardized. Vendor security questionnaires that used to vary widely now converge on a small number of common templates. SOC 2 Type II is the single most-asked-about artifact across legal, insurance, healthcare, financial services, and federal-facing buyers. Producing a current report opens conversations; missing one ends them.

2. Cyber insurance underwriting has tightened. Underwriters now condition coverage and pricing on documented compliance posture. A firm with a current SOC 2 report negotiates from a different position than one without. The premium delta and the coverage exclusions both move materially with audit posture.

3. State and industry regulation increasingly references SOC 2 as a proxy. State insurance regulators, bar associations, and healthcare oversight bodies are writing rules that either reference SOC 2 directly or align so closely with it that running a SOC 2 program also satisfies the regulatory ask. The framework that used to be optional has become operational ballast.

The firms that move first on SOC 2 are not over-investing in compliance. They are accepting that the compliance posture has become the business posture. Treating it as a routine operating function instead of a periodic project is what separates the firms that close enterprise deals from the firms that watch competitors close them.

How to Use This Checklist

Walk through the 36 items below with your team. For each item, mark one of:

- Implemented: the control is in place and you have evidence to show it.
- Partial: the control is partially in place; gaps exist.
- Missing: the control does not exist or has not been documented.

Count the implemented items. Use the scoring tiers at the end of this document to determine whether you are ready to schedule audit kickoff or still have foundational work to complete.

Save your scored checklist. Re-score quarterly so you can see whether your posture is strengthening, holding, or drifting between audit cycles.

Section 1: Governance and Ownership

The foundation of any SOC 2 program is named accountability. Without a single owner with budgeted time and the authority to hold other functions to their commitments, the program drifts.

- [ ] Compliance owner identified (single point of accountability for the SOC 2 program).
- [ ] Executive sponsor engaged and informed of audit scope and budget.
- [ ] Audit firm engaged (American Institute of Certified Public Accountants (AICPA)-licensed CPA firm).
- [ ] Audit type defined (Type 1 or Type 2) with target audit window dates.
- [ ] Internal kickoff meeting held with all control owners.
- [ ] Compliance program operating budget approved.

Section 2: Trust Services Criteria Scope

SOC 2 evaluates against the AICPA Trust Services Criteria. Security is required for every report. Availability, Processing Integrity, Confidentiality, and Privacy are optional, included only when they apply to the services you deliver.

- [ ] Trust services criteria selected (Security required; Availability, Processing Integrity, Confidentiality, Privacy as applicable).
- [ ] In-scope systems and data flows documented.
- [ ] Customer-facing services and APIs included where relevant.
- [ ] Subservice organizations identified with carve-out or inclusion approach defined.
- [ ] System description drafted in line with AICPA guidance.
- [ ] Service commitments and system requirements documented.

Section 3: Access Controls and Audit Logging

Access controls and audit logging are the most-cited finding categories in SOC 2 audits. Done well, they reduce the audit window's friction substantially. Done poorly, they extend it.

- [ ] Multi-factor authentication enforced for all production access.
- [ ] Role-based access controls aligned with least privilege.
- [ ] Quarterly access reviews documented and signed off.
- [ ] Audit logging enabled across all in-scope systems.
- [ ] Log retention meets your committed retention period (and exceeds the audit window).
- [ ] Privileged access reviewed monthly with documented justification.

Section 4: Change Management and Vendor Risk

Auditors look for evidence that production changes are controlled and that the vendors you depend on do not introduce risk you have not accepted.

- [ ] Documented change management process for production systems.
- [ ] Pull request reviews and approvals captured in audit trail.
- [ ] Production deployments logged with deployer and timestamp.
- [ ] Vendor inventory maintained with current security certifications.
- [ ] Subprocessor agreements current and reviewed annually.
- [ ] Data Processing Agreements (DPAs) signed where personal data flows to third parties.

Section 5: Incident Response and Business Continuity

The auditor will not just ask whether you have a plan. They will ask when you last exercised it, what you learned, and how the plan has changed as a result.

- [ ] Incident response plan written and reviewed in the past 12 months.
- [ ] At least one tabletop exercise conducted in the past year with documented results.
- [ ] Breach notification procedures documented (regulatory and contractual).
- [ ] Business continuity plan documented and tested.
- [ ] Backup and restore procedures tested at least quarterly.
- [ ] On-call and escalation paths documented.

Section 6: Continuous Monitoring and Evidence

The Type II report covers a continuous audit window, typically 6 to 12 months. The firms that complete Type II without scrambling are the ones that capture evidence continuously rather than reconstructing it under deadline pressure.

- [ ] Configuration drift detection running across in-scope systems.
- [ ] Vulnerability scanning on a defined cadence with findings tracked to remediation.
- [ ] Evidence collection process defined for each control.
- [ ] Risk assessment completed or updated within the past 12 months.
- [ ] Internal control monitoring or self-assessment performed at least annually.
- [ ] Control deviations documented with remediation owners and target dates.

Your 90-Day Audit-Prep Timeline

A successful Type II audit is the output of a working compliance program, not a project. The path below is the 90 days from current state to audit kickoff: the work that has to be done before you can credibly start a 6 to 12 month observation window.

The plan assumes a 25 to 100 person SMB starting from a typical Level 1 or Level 2 posture. Tighter teams move faster; larger teams move slower. The cadence is the same.

Days 1 to 30: Governance and scope

Goal: Named compliance owner with budgeted time. Audit firm engaged. Trust services criteria scope decided. System description draft underway. First evidence collection turned on.

- **Week 1:** Assign the compliance owner and document the role, time allocation, and reporting line. Brief the executive sponsor. Get the audit budget approved.
- **Week 2:** Engage two to three audit firms for proposals. Decide on Type 1 or Type 2 path. If Type 2, set the target observation window start and end dates.
- **Week 3:** Decide trust services criteria scope. Security is required; evaluate Availability, Processing Integrity, Confidentiality, and Privacy against your service commitments. Document inclusions and exclusions.
- **Week 4:** Draft the system description following the AICPA guidance. Inventory the in-scope systems, data flows, and customer-facing services. Start the subprocessor list and confirm carve-out or inclusion treatment for each.

Days 31 to 60: Controls and evidence

Goal: Access controls aligned to least privilege with quarterly review cadence in place. Audit logging baseline live across in-scope systems. Change management process documented and operating. Vendor inventory current with subprocessor agreements verified.

- **Week 5:** Run the access review across all in-scope systems. Remediate over-privileged accounts. Implement quarterly review cadence with named owners and documented sign-off.
- **Week 6:** Confirm audit logging is enabled and retained for the full audit window plus your committed retention period. Document log retention in your data retention policy. Implement monitoring that alerts when a log source goes silent.
- **Week 7:** Document the change management process. Pull request reviews, deployment approvals, and production change records all need to be capturable in audit trail. Validate the process by walking through three recent production changes.
- **Week 8:** Refresh the vendor inventory. Verify subprocessor agreements, current security certifications, and Data Processing Agreement (DPA) coverage. Triage any gaps and assign owners.

Days 61 to 90: Continuous monitoring and kickoff readiness

Goal: Continuous monitoring tuned and producing evidence as a byproduct of normal operations. Incident response and business continuity plans tested. First sample evidence package assembled and reviewed by the audit firm. Audit kickoff scheduled.

Week 9: Configure drift detection across the in-scope environment. Tune severity thresholds based on the first two weeks of alert data. Aim for under 10 percent false-positive rate before declaring the system production-ready.

Week 10: Run the first tabletop incident response exercise of the program. Document what worked, what did not, and what changes the plan needs. Test backup and restore procedures with documented results.

Week 11: Update the risk assessment. Capture identified risks, current mitigations, and accepted residual risks. Open a Plan of Action and Milestones (POA&M) for any gaps that will not be closed before kickoff. Assemble the first sample evidence package and review it with the audit firm.

Week 12: Hold the audit kickoff meeting. Confirm scope, evidence delivery method, sample sizes, and report timeline. The Type II observation window starts the day after kickoff.

By the end of 90 days, your team is not finished with compliance work. You are positioned to start the audit window with the controls operating, the evidence flowing, and the team practiced enough to maintain the cadence for the next 6 to 12 months.

Type 1 vs. Type 2: which path, and when

Many SMBs run a Type 1 audit (point-in-time control design assessment) at month 4 to confirm controls are designed correctly, then start a Type 2 observation window at month 5. The Type 1 report is a procurement bridge while the Type 2 audit window runs. Total time from current state to a usable Type 2 report: roughly 11 to 12 months. Skip Type 1 only if your enterprise buyer accepts a draft Type 2 plan plus a planned report date, or if your audit firm explicitly recommends going straight to Type 2 based on your readiness score.

Common Audit Findings and How to Avoid Them

These six findings produce more SOC 2 audit observations than any others. None of them are obscure; all of them are preventable.

1. Stale or incomplete access reviews. Access reviews that happen once a year, miss former employees, or do not produce documented sign-off are the single most common finding. Implement quarterly reviews with named owners and signature trails.

2. Audit logs that do not cover the full window. Logs that started capturing midway through the audit period, or that have gaps because a source went silent, force the auditor to extend testing or issue a qualified opinion. Implement log heartbeat monitoring and start collection well before kickoff.

3. Change management with no audit trail. Pull request reviews, deployment approvals, and production change records are all individually defensible but only collectively useful. The auditor needs to walk a sample change from request to approval to deployment to verification.

4. Vendor inventory that does not match reality. A vendor list maintained in a spreadsheet from last year is almost always wrong. Vendors with expired SOC 2 reports, missing DPAs, or undocumented data access are flagged when the auditor cross-references your inventory against the actual data flows.

5. Untested incident response and business continuity plans. A plan that exists but has never been exercised is a finding. Run a tabletop exercise with documented results. Test backups by actually restoring them.

6. Risk assessment that is more than 12 months old. A stale risk assessment signals that the program is not operating continuously. Update annually at minimum, and after any significant system or vendor change.

How to Pick Your Audit Firm

The audit firm you pick shapes the next 12 months of your program. Most SMBs pick the first firm that returns their email; the firms that pick deliberately get cleaner reports, fewer surprises, and lower bills. Eight questions to ask any candidate firm before you sign.

1. How many SMB-class clients in legal, insurance, or my specific vertical have you audited in the past 24 months?

An audit firm whose entire book is Fortune 500 will run the engagement at Fortune 500 cadence and pricing. A firm with a dozen recent SMB clients in your vertical will know what auditors look at in your kind of business. Both can produce clean reports; only one fits an SMB budget and timeline.

2. What is your pricing structure: fixed fee with milestone billing, or hourly with caps?

Fixed fee with milestone billing (kickoff, fieldwork, draft report, final report) is the SMB-friendly default. Hourly with caps can work but only if the cap is firm and the firm accepts liability for overages caused by their pace. Avoid hourly with no cap entirely.

3. What is your typical timeline from kickoff to final report?

A clean Type 1 should take 4 to 6 weeks. A clean Type 2 typically takes 3 to 4 weeks of fieldwork after the audit window closes, plus 2 to 3 weeks for the draft and final report. If a firm tells you it depends entirely on your readiness, the answer is fine; if they cannot describe a baseline timeline at all, that is a signal.

4. Who will be the lead auditor on my engagement, and can I speak with them before signing?

The lead auditor's experience is the single biggest predictor of your engagement quality. Ask for at least 3 years of SOC 2 audit experience and confirm the named individual will be on every major call. Firms that rotate lead auditors mid-engagement are firms with retention problems; that becomes your problem.

5. What is your remediation philosophy when you find a control gap during fieldwork?

Strong firms flag gaps early enough that you can remediate before they appear in the report. Weak firms (or rigid firms) document everything as a finding regardless of remediation status. The difference matters for

procurement; ask for examples of how recent gaps were handled.

6. What evidence collection methods do you accept?

Live read-only access to your evidence platform is the lowest-friction path; emailed PDFs are the highest-friction. Confirm the firm accepts what you have. If you have a compliance automation platform (Drata, Vanta, Secureframe, Tugboat Logic, or similar), confirm the firm has worked with it before.

7. What is your communication cadence during the audit window?

Weekly status with named blockers is the SMB-friendly default. Monthly is too sparse; daily is too dense. Confirm there is a named point of contact at the firm during the entire audit window.

8. Can you provide three SMB-class references with current contact information?

References are only useful if you can call them. A firm that gives you three named clients in your size class and willingly takes a 30-minute call from you is a firm with strong client relationships. A firm that resists, anonymizes, or only offers logos is a firm with something to hide.

Red flags

- Pricing is "we will quote after kickoff" with no published structure.
- No SMB-tier references; only enterprise.
- Lead auditor not named, or rotated each engagement.
- No upfront evidence-request list provided.
- Out-of-band billing for "additional testing" without prior approval.
- More than a 6-week gap between fieldwork and draft report.

Green flags

- Published fixed-fee schedule with optional add-ons clearly priced.
- Named lead auditor with 3+ years SOC 2 experience and at least one prior client in your vertical.
- Pre-audit readiness assessment offered as a separate, smaller engagement.
- Sample evidence-request list provided before contract is signed.
- Annual fee held flat or reduced for clean Year 2 audits.
- SMB-class reference customer willing to take a 30-minute call.

Big-Four vs. boutique vs. mid-tier

Big-Four firms (Deloitte, EY, KPMG, PwC) put a recognizable brand on your report; some procurement teams require it. Boutique firms specialize in SOC 2 for SMBs, typically offer better client service, but their brand may be unfamiliar. Mid-tier firms sit in between and are usually the best fit for SMBs serving enterprise customers. Pricing tends to scale 1.5 to 2x from boutique to Big-Four for the same scope.

What SOC 2 Actually Costs

The single most-asked, least-answered question in SOC 2 conversations: what does it cost? The numbers below describe the typical SMB range. Your specific cost depends on TSC scope, environment complexity, audit firm, and whether you buy a compliance platform.

Audit firm fees (the biggest line item)

Type 1 audit (Security TSC only): $15,000 to $30,000
Higher with multiple TSC criteria; usually fixed fee with milestone billing.

Type 2 audit (Security TSC only): $25,000 to $60,000
Driven by audit window length (6 vs 12 months), in-scope environment complexity, and firm size.

Type 2 with multiple TSC criteria: $45,000 to $100,000+
Each additional TSC criterion (Availability, Confidentiality, Processing Integrity, Privacy) adds testing scope and typically 15 to 25 percent to the fee.

Compliance platform fees (optional but common)

SMB-tier compliance automation platform: $10,000 to $30,000 per year
Drata, Vanta, Secureframe, Tugboat Logic, and similar. Heavily reduces internal time on evidence collection.

Cloud-native equivalent (AWS Audit Manager + Config + custom): $5,000 to $15,000 per year
Lower cost; higher internal expertise required to configure and maintain.

Internal time investment

Compliance owner: 25 to 50 percent of one Full-Time Equivalent (FTE) during prep; 10
Often a fractional Chief Information Security Officer (CISO) at SMB scale.

Engineering team: 80 to 120 hours initial setup; 10 to 20 hours per quarter ongoing
Concentrated in Phase 1 of the 90-day plan, then much lighter.

Executive sponsor: 4 to 8 hours per quarter
Reviews program metrics, signs off on risk decisions, attends auditor calls.

Year 1 vs. ongoing

Year 1 total SMB budget (typical): $40,000 to $120,000
Setup work, first audit cycle, learning curve.

Year 2 and beyond (typical): $30,000 to $80,000 per year
Roughly 60 to 70 percent of Year 1 cost as the program matures and findings reduce.

What pushes the number up

- Multiple TSC criteria selected at the start instead of phased.
- Complex multi-cloud or hybrid architecture in scope.
- Many in-scope subprocessors requiring carve-out or inclusion treatment.
- Findings during audit that extend the window or require re-testing.
- Attempting Type 2 without first running a readiness assessment or Type 1.

Path to lower cost

- Start with Security TSC only; add other criteria when contractually required.
- Use cloud-native compliance services before buying a third-party platform.
- Schedule the audit window to align with calendar simplicity (single fiscal year).
- Run a pre-audit readiness assessment 90 days before kickoff to surface gaps cheaply.
- Build internal compliance owner capacity before paying for a fractional CISO.

What an Evidence Package Looks Like

Auditors do not want to receive emails with 50 PDFs. They want a single organized package mapped to control families with consistent file naming and timestamps that fall inside the audit window. The folder structure below is what most SMBs end up with after one or two audit cycles; starting with it saves you the cycles.

Folder structure

```
SOC2-Type2-EvidencePackage-2026/
|-- 00-System-Description/
|   |-- system-description-v2.pdf
|   `-- data-flow-diagram.pdf
|-- 01-Governance/
|   |-- compliance-owner-charter.pdf
|   `-- kickoff-minutes.pdf
|-- 02-Access-Control/
|   |-- access-policy-v3.2.pdf
|   |-- q1-2026-review-signed.xlsx
|   `-- mfa-screenshot-Q1.pdf
|-- 03-Change-Management/
|   |-- change-mgmt-policy.pdf
|   |-- deployment-log-Q1.csv
|   `-- sample-tickets-Q1.zip
|-- 04-Audit-Logging/
|   |-- log-retention-policy.pdf
|   `-- cloudtrail-config.pdf
|-- 05-Vendor-Management/
|   |-- vendor-inventory-2026.xlsx
|   |-- soc2-reports-current/
|   `-- dpa-coverage-matrix.pdf
|-- 06-Incident-Response/
|   |-- ir-plan-v4.pdf
|   `-- tabletop-Q2-results.pdf
|-- 07-Business-Continuity/
|   |-- bcp-plan.pdf
|   `-- restore-test-Q1.pdf
|-- 08-Risk-Management/
|   |-- risk-assessment-2026.pdf
|   `-- poam-current.xlsx
`-- 09-Continuous-Monitoring/
    |-- drift-detection.pdf
    `-- monthly-effectiveness/
```

File naming conventions

- Lowercase-hyphenated names. No spaces or special characters.
- Include version numbers for evolving documents (policy-v3.2.pdf).
- Include period markers for time-bounded artifacts (q1-2026-access-review.xlsx).
- Standardize date format (YYYY-MM-DD or YYYY-Q1 through Q4).
- Consistent extensions: .pdf for policies, .xlsx for exported data, .csv for raw exports.

What goes in each folder

- Policies and procedures: PDF with version number.
- Configuration screenshots: PDF or PNG, dated within the audit window.
- Exported logs or reports: CSV or XLSX with export timestamp in filename.
- Sample tickets or change records: ZIP if multiple, otherwise individual PDFs.
- Retain originals; do not redact unless contractually required.

What auditors prefer

- Live read-only access to your evidence platform OR a single shared cloud folder.
- Single source of truth; avoid emailing PDFs back and forth.
- Files dated within the audit window; historical context clearly tagged.
- Documentation of when each artifact was generated and by whom.

Scoring

Total possible: 36 items implemented.

30 to 36 items	Audit-ready. Schedule kickoff with confidence.
22 to 29 items	Foundations are forming, but address remaining gaps before kickoff to avoid extending the audit window or receiving a qualified opinion.
Below 22 items	Significant gaps. Start with governance, scope, and evidence collection before engaging an auditor.

A firm scoring 30 or higher will not be common on first pass. That is intentional. The bar is calibrated to identify the firms ready to start a Type II window without scrambling, not to clear every team that has read the framework.

Printable Scoring Sheet

Print this page. Take it to a conference room. Walk through the 36 items with the team and mark each one. The page is designed to live on a wall or in a binder for the duration of your prep.

1. Governance and Ownership

- ☐ Compliance owner identified _____
- ☐ Executive sponsor engaged _____
- ☐ Audit firm engaged (AICPA-licensed) _____
- ☐ Audit type defined (Type 1 or Type 2) _____
- ☐ Internal kickoff meeting held _____
- ☐ Compliance program budget approved _____

2. Trust Services Criteria Scope

- ☐ TSC selected (Security required) _____
- ☐ In-scope systems and data flows documented _____
- ☐ Customer-facing services included _____
- ☐ Subservice organizations identified _____
- ☐ System description drafted _____
- ☐ Service commitments documented _____

3. Access Controls and Audit Logging

- ☐ MFA enforced for all production access _____
- ☐ Role-based access aligned with least privilege _____
- ☐ Quarterly access reviews documented _____
- ☐ Audit logging across in-scope systems _____
- ☐ Log retention exceeds audit window _____
- ☐ Privileged access reviewed monthly _____

4. Change Management and Vendor Risk

- ☐ Documented change management process _____
- ☐ PR reviews captured in audit trail _____
- ☐ Production deployments logged _____
- ☐ Vendor inventory current _____
- ☐ Subprocessor agreements current _____
- ☐ DPAs signed for personal data flows _____

5. Incident Response and Business Continuity

- ☐ IR plan reviewed in past 12 months _____
- ☐ Tabletop exercise documented in past year _____
- ☐ Breach notification procedures documented _____
- ☐ BCP documented and tested _____
- ☐ Backup and restore tested quarterly _____
- ☐ On-call and escalation paths documented _____

6. Continuous Monitoring and Evidence

- [ ] Configuration drift detection running _____
- [ ] Vulnerability scanning on defined cadence _____
- [ ] Evidence collection process per control _____
- [ ] Risk assessment updated past 12 months _____
- [ ] Internal control monitoring annual _____
- [ ] Control deviations tracked in POA&M _____

Total implemented (out of 36): _____

30 to 36: Audit-ready. Schedule kickoff.
22 to 29: Foundations forming; address gaps before kickoff.
Below 22: Significant gaps; start with governance, scope, and evidence collection.

A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business and an Amazon Web Services (AWS) Advanced Tier Partner with a Defense Counterintelligence and Security Agency (DCSA) Secret-level Facility Clearance and Cybersecurity Maturity Model Certification (CMMC) Level 2 self-assessment status. We help regulated SMBs across legal, insurance, healthcare, financial services, and federal verticals build SOC 2-ready cloud environments and operate them through every audit window.

If you are using this checklist to assess your own readiness and want a second set of eyes on your scoring, or if you are pursuing SOC 2 alongside HIPAA or state insurance regulation alignment, we are happy to help.

For the architectural foundation this checklist presumes, the Cloud Landing Zones Guide is our 28-page tactical playbook for compliance-first multi-account architecture. SOC 2 Type II requires logical separation between production and non-production environments; the Guide walks through how to build that separation by design so the auditor's evidence requests map onto the architecture rather than triggering remediation. Free at pandoracloud.net/cloud-landing-zones-guide.

Ready for a second set of eyes on your scoring?

Schedule a free 30-minute consultation. We will walk through your scored checklist and help you prioritize the next 90 days.

pandoracloud.net/#schedule-consultation

Glossary

For readers new to SOC 2 vocabulary, this glossary names the most common terms referenced in this checklist.

AICPA (American Institute of Certified Public Accountants)
The professional body that defines the SOC 2 audit framework and licenses CPAs to perform the audits.

Audit Window
The continuous period of time covered by a Type II report, typically 6 to 12 months. Controls must operate effectively across the full window, not just at a point in time.

Carve-out vs Inclusion
Two approaches to handling subservice organizations in your SOC 2 report. Carve-out treats them as out of scope; inclusion brings them into the audit.

DPA (Data Processing Agreement)
Contract that governs how a third party handles personal data on your behalf. Required under most modern privacy regulations.

POA&M (Plan of Action and Milestones)
Structured tracking of known gaps with owners, deadlines, and remediation status. Demonstrates that you recognize and manage gaps rather than hide them.

Subservice Organization
A vendor or service provider whose controls are relied upon as part of your environment. Cloud providers, managed service providers, and outsourced operations all qualify.

Type 1 Report
Auditor confirms that controls are designed correctly on a single date. Useful as a stepping stone but rarely sufficient for enterprise procurement.

Type 2 Report
Auditor tests whether controls operated effectively across the audit window. The version enterprise buyers actually want to see.