SOC ESSENTIALS

SOC Myths Corrected, Best Practices Defined, Key Terms Explained

A Practical Reference





Perkins & Co



Fintech Community

Technology Association of Oregon

techoregon.org/communities/fintech

A Practical Reference for Navigating SOC Reports, Controls, and Expectations

SOC ESSENTIALS

A Practical Reference

TABLE OF CONTENTS

Myths	3
Best Practices	7
Key Terms	8
Compare SOC 1 & 2	15

SOC Essentials brings clarity to one of the most misunderstood areas of technology and compliance.

This guide corrects widespread SOC myths, defines the best practices that drive successful audits, and explains the key terms leaders must understand.

Whether you are preparing for your first SOC report or maturing an existing program, this resource delivers the knowledge needed for confident, informed decision-making.

tao Perkins & Co

Perkins & Co

Perkins & Co, Portland's largest locally-owned accounting firm and AICPA-licensed CPA practice, provides comprehensive SOC 1, SOC 2, and SOC 3 audit services. With extensive technology risk expertise and consultative approach, they help service organizations demonstrate security, compliance, and trustworthiness to customers.

TAO /Fintech

TAO /Fintech is a burgeoning professional community designed to bring together and unite individuals and organizations across the Fintech Ecosystem for support, connection, growth and expansion.

Fintech Community

Technology Association of Oregon

techoregon.org/communities/fintech

Myths *Corrected*



This section breaks down the most common misconceptions about SOC audits, replacing confusion with clarity. Each Myth is corrected with concise, practical insight that helps organizations understand what SOC really requires, what it doesn't, and how to avoid costly misunderstandings.

MYTH 1

SOC 2 is a Certification

The Reality

SOC 2 isn't a certification, it's an attestation. A CPA issues an opinion, not a seal of approval. It's a report card, not a trophy.

Why This Matters

Calling it a certification misleads customers and sets unrealistic expectations. Use the right language to preserve trust and credibility.

MYTH 2

SOC 2 is a Pass/Fail Test

The Reality

There is no pass or fail. SOC reports issue opinions: unqualified, qualified, adverse, or disclaimer. Exceptions don't mean failure, they mean transparency.

Why This Matters

Customers often misunderstand the presence of exceptions. Educating them helps ensure the report is used properly and prevents panic over a minor exception.

MYTH 3

A SOC Audit Covers the Entire Company

The Reality

SOC reports evaluate systems, not entire companies. Many organizations need multiple SOC reports because they operate multiple systems, platforms, or business lines.

Why This Matters

If you lump everything together to save money, you risk exposing irrelevant deficiencies to customers who don't use that part of your business and confusing the entire audience.

MYTH 4

SOC Engagements Are One-Size-Fits-All

The Reality

Scope varies widely: systems, processes, criteria, risk levels, data types, and customer commitments all influence the design of a SOC audit.

Why This Matters

Organizations that assume a generic approach end up mis-scoped, mis-budgeted, and surprised. Tailoring the engagement is essential.



MYTH 5

SOC 2 is a One-Time Achievement

The Reality

SOC 2 Type 2 covers a period of time, requires ongoing control monitoring, and m be renewed annually.

Why This Matters

Security isn't static. Treating SOC as a checkbox instead of a continuous commitment leads to degraded controls, audit failures, and customer distrust.

MYTH 6

I Don't Need to Worry About SOC Until Someone Asks

The Reality

By the time a customer asks for a SOC 2, you're already behind. Developing controls, gathering evidence, refining processes, and completing a Type 2 period takes months.

Why This Matters

Organizations lose deals because they need a SOC report now. Early preparation is a competitive advantage, and delays can kill opportunities.

MYTH 7

SOC 2 Type 2 Must Cover a Full Year

The Reality

There is no required minimum period in the standards. Many first-time Type 2 reports cover 3 to 6 months, though longer periods are preferred once controls mature.

Why This Matters

Believing you must wait 12 months stops companies from beginning early and delays market readiness unnecessarily.

MYTH 8

SOC 2 Only Applies to Large Companies

The Reality

Even the smallest organizations, including two-person companies, can achieve SOC 2. It's not about size, it's about risk, data sensitivity, customer commitments, and control structure.

Why This Matters

Startups often assume they are too small, delaying critical control development and losing out on enterprise deals.



MYTH 9

SOC 2 Only Covers IT Security

The Reality

A large portion of SOC 2 has nothing to do with firewalls or servers. The COSO framework requires governance, culture, tone-at-the-top, HR processes, risk assessment, communication, and more.

Why This Matters

Most new clients think they're ready because they've locked down IT. Governance-level controls take time and are a common source of exceptions.

MYTH 10

All Five Trust Services Categories are Included Automatically

The Reality

Only Security is mandatory. Availability, Processing Integrity, Confidentiality, and Privacy are optional, but your customer commitments and contract language should drive your selections.

Why This Matters

If you promise 99.9 percent uptime, customers expect Availability in your SOC 2. Missing it creates misalignment and credibility gaps.

MYTH 11

SOC Reports are Basically All the Same

The Reality

SOC follows a shared framework, but auditor wisdom, experience, scoping decisions, system boundaries, and testing depth vary dramatically.

Why This Matters

A low-quality SOC report is worse than having none. Enterprise buyers scrutinize the details and the audit firm behind it.

MYTH 12

An Unmodified Report Means There Were No Issues

The Reality

Auditors test samples, sometimes less than 1 percent of transactions. Unmodified means controls were effective, not perfect.

Why This Matters

Organizations and customers may assume clean equals flawless. SOC provides reasonable assurance, not absolute certainty.



MYTH 13

Penetration Testing is Optional and Unrelated to SOC

The Reality

While not literally required, pen tests support key SOC controls such as vulnerability management and incident response. Customers frequently expect them.

Why This Matters

Skipping pen tests weakens your security posture, creates audit surprises, and raises red flags with enterprise buyers.

MYTH 14

My Controls Don't Need to Change Once Written

The Reality

Controls must evolve as systems, workflows, personnel, and risks evolve. A control written two years ago may no longer reflect reality.

Why This Matters

Static controls fail Type 2 audits. Untracked changes in technology or process often lead to six months of failed testing.

MYTH 15

A SOC Engagement Has Nothing to Do with Customer Contracts

The Reality

Your customer commitments drive SOC expectations. If your contracts or website promise confidentiality, uptime, or processing accuracy, your SOC scope should reflect these commitments.

Why This Matters

Misalignment between your public promises and your SOC categories makes reports look incomplete or misleading.

MYTH 16

Automation Doesn't Matter, Manual Controls are Fine

The Reality

Manual controls frequently fail. Automated and centralized workflows significantly improve consistency, timing, and evidence quality.

Why This Matters

Organizations that rely on email reminders, spreadsheets, or local staff often experience repeated audit exceptions. Automation increases reliability.

Best Practices *Defined*



This section outlines proven Best Practices that strengthen SOC readiness and audit performance. Each Practice offers practical, actionable guidance for designing effective controls, aligning scope, improving consistency, and building a program that operates reliably throughout the audit period and earns customer trust.

PRACTICE 1

Scope to the System, Not the Company

SOC reports are issued on systems, not organizations. Define clear system boundaries that match how services are delivered to customers. Narrow scope reduces complexity, eliminates irrelevant controls, and produces a report that is far more meaningful to report users.

PRACTICE 2

Align Scope with Customer Expectations

Review contracts, SLAs, and customer-facing commitments to ensure selected Trust Services Criteria accurately reflect what you promise. Aligning scope with commitments avoids gaps, credibility issues, and report limitations that may concern customers or delay sales.

PRACTICE 3

Strengthen Entity-Level Controls Early

One-third of SOC 2 Common Criteria relate to governance, ethics, and tone-at-the-top. Establish clear policies, decision-making processes, HR practices, and communication channels early, as these foundational controls heavily influence audit outcomes and organizational maturity.

PRACTICE 4

Conduct a Formal Risk Assessment, Annually

A thoughtful, documented risk assessment is central to SOC 2. Evaluate threats, business changes, vendor dependencies, and control effectiveness. A strong risk assessment informs scoping decisions, identifies control gaps, and ensures your SOC 2 program stays relevant as your environment evolves.



PRACTICE 5

Centralize and Automate Key Controls

Automate recurring controls wherever possible, especially provisioning, deprovisioning, review cycles, and change approvals. Automation reduces human error, improves evidence quality, and dramatically increases consistency across the audit period, lowering the likelihood of exceptions.

PRACTICE 6

Integrate Change Management with SOC Controls

System or process changes must flow directly into SOC control documentation. Document changes as they occur and ensure downstream controls are updated. Change management alignment prevents outdated controls, silent failures, and exceptions in Type 2 audits.

PRACTICE 7

Build the Control Set Before Audit Kickoff

Well-defined controls streamline the audit and reduce cost. Design the control set, assign owners, ensure execution, and gather sample evidence before auditors begin. Entering the exam with mature, well-understood controls leads to smoother testing and predictable timelines.

PRACTICE 8

Prepare the System Description Early

Drafting the system description in advance clarifies scope, dependencies, boundaries, and commitments. Early preparation reduces rework, prevents scope confusion, and accelerates the readiness phase, ensuring the final report accurately reflects your environment.

PRACTICE 9

Evaluate Trust Services Criteria Thoughtfully

Security is mandatory, but additional criteria should be included when they support customer commitments or data processing activities. Review each criterion against your environment to determine whether Availability, Privacy, Confidentiality, or Processing Integrity add necessary assurance.



PRACTICE 10

Use Points of Focus to Guide Control Design

The AICPA Points of Focus offer clear guidance on what strong controls should demonstrate. Reviewing these for each Common Criterion helps identify missing controls, adapt to organizational changes, and ensure your program remains aligned with SOC expectations.

PRACTICE 11

Maintain Documentation Continuously, Not Annually

Documentation should evolve in step with the environment. Keep policies, workflows, diagrams, inventories, and narratives updated throughout the year. Continuous documentation prevents last-minute scrambles and strengthens evidence quality for the full audit period.

PRACTICE 12

Assess Vendor Risk and Third-Party Dependencies

SOC 2 requires understanding risks introduced by vendors and partners. Maintain an updated vendor inventory, review SOC reports where appropriate, and document how outsourced activities impact your service commitments and system boundaries.

PRACTICE 13

Establish Clear Evidence Collection Processes

Create repeatable, centralized procedures for collecting and storing audit evidence. Use tooling or shared repositories to ensure evidence is complete, consistent, timestamped, and accessible. Strong evidence workflows reduce friction and shorten the audit cycle.

PRACTICE 14

Monitor Organizational Changes Throughout the Year

Track leadership changes, new systems, new product lines, restructuring, and policy updates. Organizational shifts regularly impact SOC controls. Monitoring these proactively helps maintain accurate control design and prevent audit-time surprises.



PRACTICE 15

Communicate Control Responsibilities Across Teams

SOC controls typically span engineering, HR, security, finance, and operations. Clearly define roles, ownership, and expectations, and ensure cross-functional teams understand their part in maintaining compliance throughout the year.

PRACTICE 16

Validate Readiness Before Starting Type 2

Before entering a Type 2 period, confirm controls are designed, consistently executed, and supported by evidence. A structured readiness review avoids avoidable exceptions and ensures the first Type 2 report reflects real operational maturity.

PRACTICE 17

Conduct Annual Policy and Procedure Reviews

Policies must reflect actual practice. Update policies to match current workflows, technologies, and staffing models. Annual reviews ensure alignment between documented expectations and real-world execution across the audit period.

PRACTICE 18

Prioritize Consistency Over Complexity

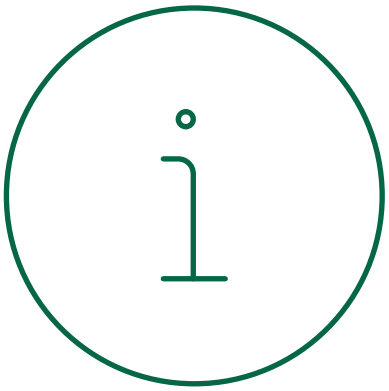
Simple, consistent controls outperform complex, inconsistent ones. Focus on clarity, repeatability, and reliability. Controls should match your operating reality, not introduce unnecessary burden or risk accidental failure.

PRACTICE 19

Engage Your Auditor as a Strategic Partner

Auditors bring perspective across industries and maturity levels. Maintain open communication, share system changes, and ask clarifying questions. A collaborative relationship leads to smoother audits and helps organizations mature more quickly.

Key Terms *Explained*



These Key Terms helps to clarify the essential concepts, and language used in SOC audits. Designed for clarity and accessibility, it helps teams understand key definitions, reduce confusion, and speak confidently about controls, criteria, evidence, assurance, and the core elements that shape every SOC examination.

AICPA

The American Institute of Certified Public Accountants. The AICPA establishes the professional standards that govern SOC examinations, including the Trust Services Criteria, the structure of SOC reports, and the requirements auditors must follow when issuing attestation opinions. All SOC 1, SOC 2, and SOC 3 reports are performed under AICPA standards.

Attestation

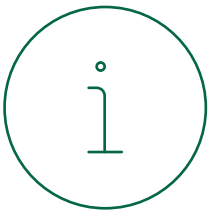
An independent auditor's opinion on whether controls were designed and operated effectively. It is not a certification. It is a formal, evidence-based conclusion about a system's security and reliability.

Common Criteria

The base-level criteria, drawn from the Trust Services Criteria, that every SOC 2 report must address when evaluating the Security category. They cover governance, risk assessment, communication, monitoring, and control activities.

Complementary User Entity Controls (CUECs)

Controls that the customer (the user entity) must perform for the service organization's controls to function as intended. These appear in most SOC reports.



Control

A specific policy, procedure, or activity designed to manage risk and ensure the system meets its commitments. Controls can be technical (automated) or administrative (manual).

Control Attribute

The underlying characteristic of a control, such as frequency, precision, purpose, or evidence source. Attributes determine whether a control can be tested and how effective it is.

Control Automation

Use of technology to perform controls consistently. Automation reduces human error and strengthens evidence quality.

Control Design vs. Control Operation

Design: Whether the control is appropriate and complete.

Operating Effectiveness: Whether the control actually functioned consistently over time.

SOC Type 2 evaluates both.

Control Environment

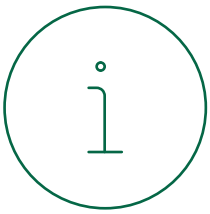
The governance layer of SOC 2. Includes leadership, ethics, policies, HR practices, authority structures, communication expectations, and overall cultural commitment to doing things the right way.

COSO Framework

A widely used internal control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission. COSO defines five components of effective internal control, including governance, risk assessment, communication, monitoring, and control activities. SOC 2 incorporates COSO principles as the foundation for evaluating organizational controls beyond technical security.

Entity-Level Controls

Controls applied across the entire organization, not specific systems. Examples include security policies, HR processes, governance practices, risk management, and monitoring activities.



Evidence

Documentation, logs, screenshots, reports, tickets, approvals, or artifacts used to demonstrate that a control operated correctly. Evidence must be consistent with the control's frequency and precision.

Exception

A deviation where a control did not operate as designed or expected during the audit period. Exceptions do not automatically mean failure. They identify areas for improvement and help customers understand operational risk.

Governance Controls

Controls that reflect leadership behaviors, expectations, and oversight. These include policies, ethics codes, oversight committees, and accountability structures.

Materiality

A concept determining whether an exception or deficiency is significant enough to impact the auditor's opinion. Minor issues may not affect the overall report.

Modified / Unmodified Opinion

Unmodified means the auditor concluded the controls were effective.

Modified means there were qualifications, limitations, or material exceptions.

Neither is "pass" or "fail," but they affect how customers interpret the report.

Penetration Test

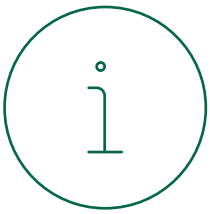
A structured attempt to exploit vulnerabilities in your systems. While not explicitly required, pen tests often support vulnerability management and incident response expectations in SOC 2.

Points of Focus

Guidance provided by the AICPA that explains what strong controls should look like under each criterion. Points of Focus help organizations design controls and help auditors determine if they are appropriate.

Principal Service Commitment

A documented promise your company makes to customers about how their data will be handled. These commitments influence which Trust Services Criteria must be included in the SOC scope.



Reasonable Assurance

The level of confidence SOC audits provide. It is strong and reliable, but not absolute. Controls may still fail or miss events outside the audit sample.

Risk Assessment

A formal process for identifying threats, evaluating impact/likelihood, and determining how risk will be mitigated. Risk assessments directly influence SOC scoping and control design.

System Boundary

The defined scope of what is included in the SOC report: the system, processes, infrastructure, data flows, tools, and components used to deliver the service. SOC reports are about the system, not the entire company.

Trust Services Criteria (TSC)

The framework used for SOC 2 evaluations. The five categories are Security (required), Availability, Processing Integrity, Confidentiality, and Privacy. Organizations choose which TSC apply based on commitments and risks.

Type 1 Report

A SOC report that evaluates whether controls were suitably designed and implemented at a point in time. It is a snapshot of readiness, not ongoing effectiveness.

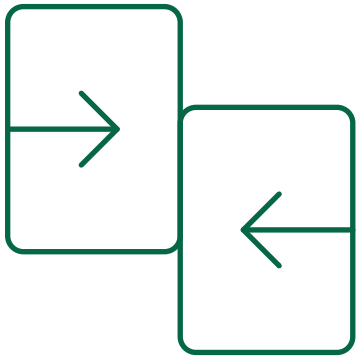
Type 2 Report

A SOC report that evaluates whether controls operated effectively over a defined period (typically 6–12 months). It demonstrates sustained performance, not just design.

Vulnerability Scan

Automated scanning tools that identify known weaknesses in systems. These scans are often recurring controls tested as part of SOC evaluations.

Compare *Grid*



This comparison grid clearly outlines the differences between SOC 1 and SOC 2, detailing each report's purpose, focus, and audience. It helps organizations quickly determine which examination aligns with their services, customer expectations, and compliance needs, ensuring confident and informed selection.

ID	ELEMENT	SOC 1	SOC 2
1	**Focus**	Financial reporting controls	Security, availability, processing integrity, confidentiality & privacy
2	**Primary Purpose**	Assurance over controls affecting client financial statements	Assurance over security and data protection controls
3	**Audience**	Client auditors, financial statement preparers	Customers, prospects, business partners, regulators
4	**Distribution**	Restricted (under NDA)	Restricted (under NDA)
5	**Detail Level**	High - includes control descriptions, testing procedures, and results	High - includes control descriptions, testing procedures, and results
6	**Report Types Available**	Type I (point in time) & Type II (period of time)	Type I (point in time) & Type II (period of time)
7	**Time Period Covered**	Type I: Single point in time Type II: Minimum 6 mos (typically 6-12 mos)	Type I: Single point in time Type II: Minimum 3-6 mos (typically 6-12 mos)
8	**Best For**	Payroll processors, claims processors, loan servicers, any service affecting client financials	SaaS companies, cloud providers, data centers, MSPs, healthcare tech
9	**Trust Services Criteria**	Not applicable (focuses on financial controls)	Security (required) + optional: Availability, Processing Integrity, Confidentiality, Privacy
10	**Renewal Frequency**	Annually	Annually
11	**Can Be Used For**	Satisfying client auditor requirements, regulatory compliance	Customer security questionnaires, RFP responses, enterprise sales
12	**Prerequisites**	Documented financial controls, evidence of operation	Comprehensive security program, documented policies and procedures

SOC ESSENTIALS

A Practical Reference for Navigating SOC Reports, Controls, and Expectations

