Preparing for a SOC Audit: A Project Manager's Guide to Success

Welcome to this comprehensive guide on navigating System and Organization Controls (SOC) audits. As project managers, we often find ourselves coordinating complex compliance initiatives that require cross-functional collaboration and meticulous planning.

This presentation will equip you with practical strategies, tools, and insights to successfully lead your organization through the SOC audit process, from initial preparation to final certification.

kW by Kimberly Wiethoff

Understanding SOC Audit Types

SOC 1

Focuses on controls relevant to financial reporting

Designed for service organizations that impact client financial statements

Reports are restricted to management, customers, and auditors

SOC 2

Examines controls related to the Trust Service Criteria

Addresses security, availability, processing integrity, confidentiality, and privacy

More comprehensive security assessment than SOC 1

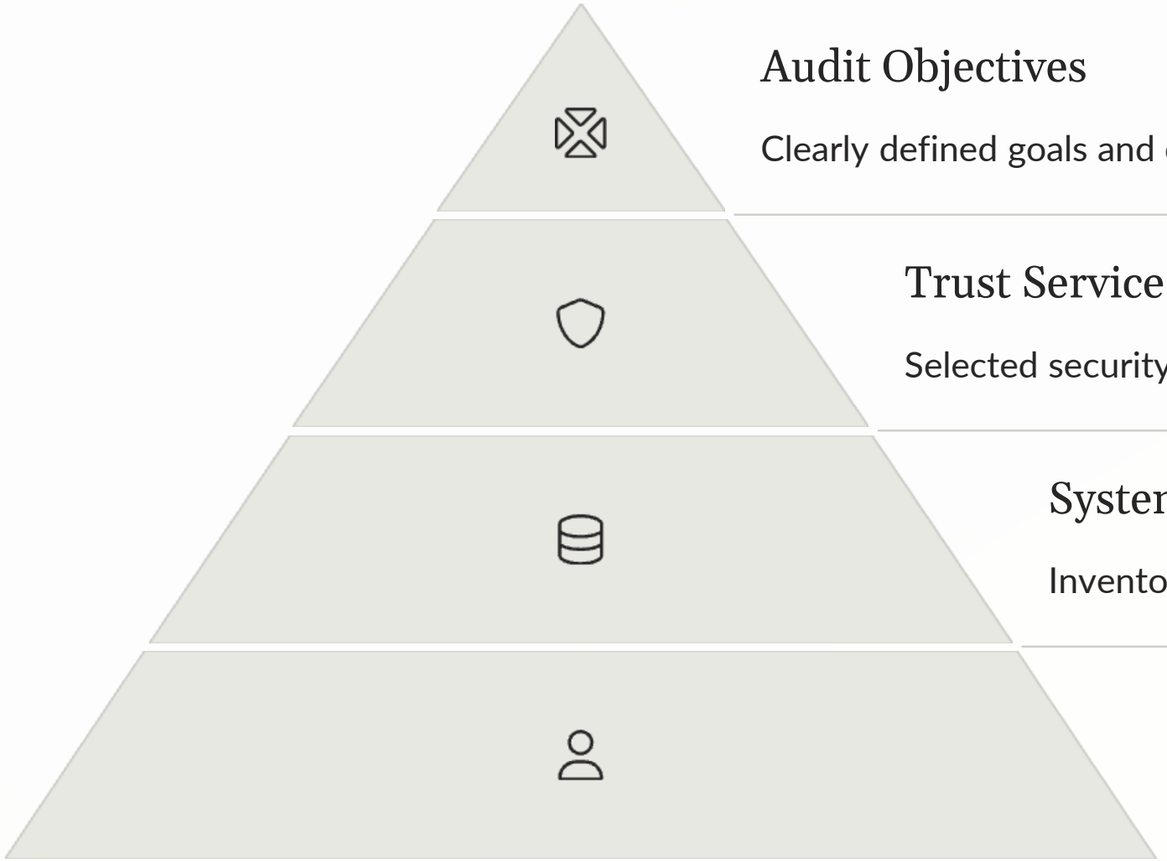
SOC 3

Contains the same criteria as SOC 2

Simplified report format without sensitive details

Can be freely distributed to the public as a marketing tool

Defining Your SOC Audit Scope



Audit Objectives

Clearly defined goals and compliance targets

Trust Service Criteria

Selected security principles and requirements

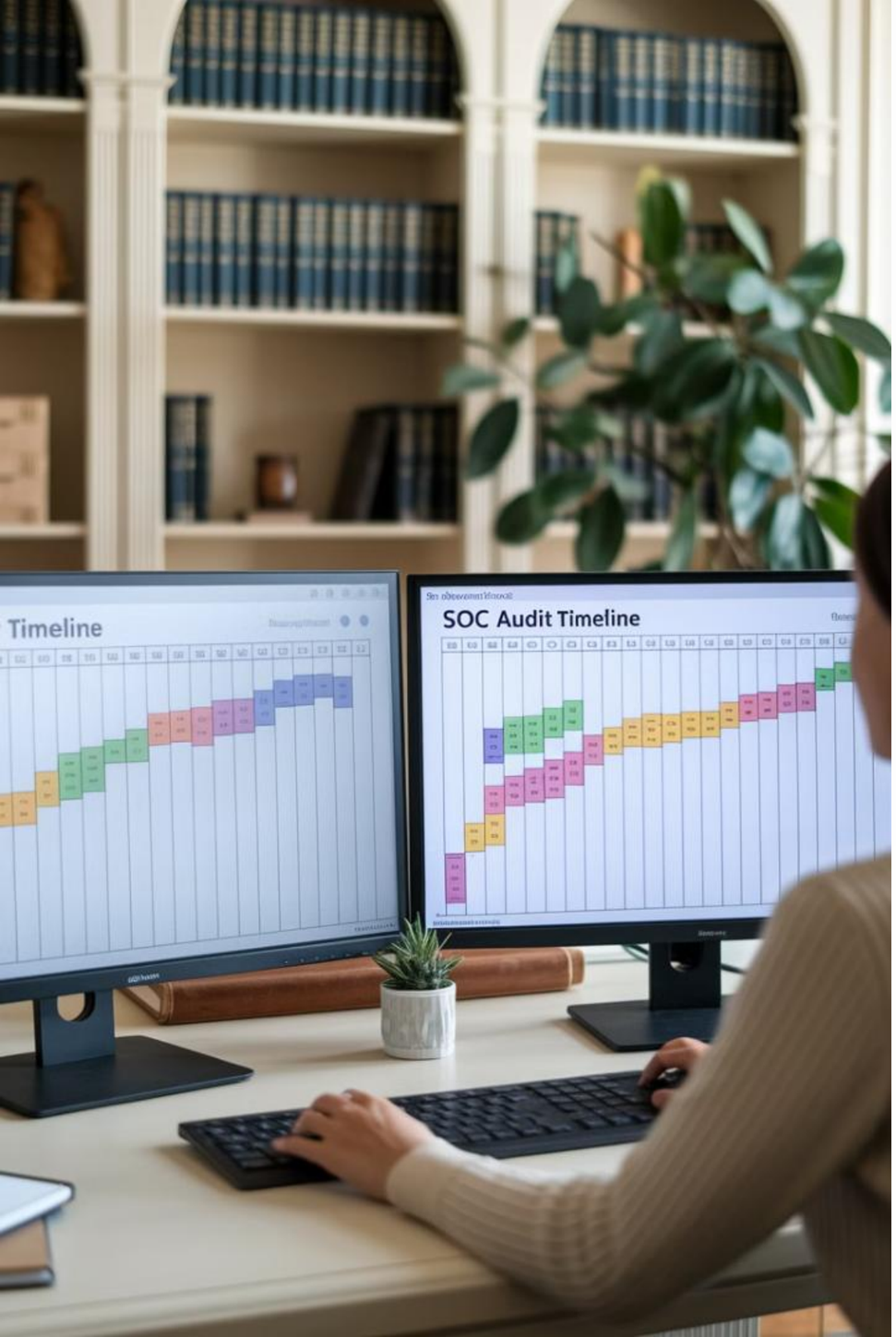
Systems & Applications

Inventory of in-scope technologies

People & Processes

Teams, vendors, and workflows involved

The scope of your SOC audit determines everything from resource allocation to timeline. Work with your compliance and security teams to precisely define which systems, data, processes, and trust criteria will be included. Document all boundaries and exclusions to prevent scope creep during the audit process.



Building Your Audit Project Plan

Initiation

- Define objectives
- Identify stakeholders
- Secure resources

Planning

- Develop timeline
- Create RACI matrix
- Set milestones

Execution

- Collect evidence
- Review controls
- Address gaps

Completion

- Final review
- Auditor sessions
- Report issuance

Work backward from your audit deadline to create a comprehensive timeline with buffer periods for unexpected issues. Ensure your plan addresses resource constraints and accounts for competing priorities across teams.

Creating Your SOC Audit RACI Matrix

Activity	IT Security	HR	DevOps	Legal	Project Manager
Access Control Documentation	R	C	C	I	A
Incident Response Testing	R	I	C	C	A
HR Employee Screening	I	R	I	C	A
Change Management Evidence	C	I	R	I	A
Vendor Risk Assessments	C	I	I	R	A

A well-defined RACI matrix eliminates confusion about who is Responsible for executing tasks, who is Accountable for results, who needs to be Consulted before decisions, and who should be Informed of progress. This clarity is crucial for the cross-functional nature of SOC audits.

Review this matrix with all stakeholders to ensure alignment and buy-in before evidence collection begins. Update it as responsibilities shift throughout the project.

Evidence Collection Best Practices

Build a Centralized Repository

- Use SharePoint, Confluence, or dedicated GRC tools
- Implement clear folder structures with naming conventions
- Set appropriate access controls for sensitive evidence

Standardize Evidence Format

- Create templates for screenshots and narratives
- Include dates, systems, and control references
- Redact sensitive data before sharing with auditors

Track Submission Status

- Maintain a real-time evidence tracking dashboard
- Send automated reminders for outstanding items
- Escalate delayed submissions to leadership

Evidence quality can make or break your audit. Ensure all screenshots include timestamps, usernames (sanitized if necessary), and system identifiers. For recurring evidence, collect samples across the entire audit period to demonstrate consistent control operation.

Common Evidence Requirements

Risk Management

- Vulnerability scans
- Risk assessments
- Mitigation plans

Change Management

- Approval workflows
- Testing documentation
- Implementation plans

Infrastructure

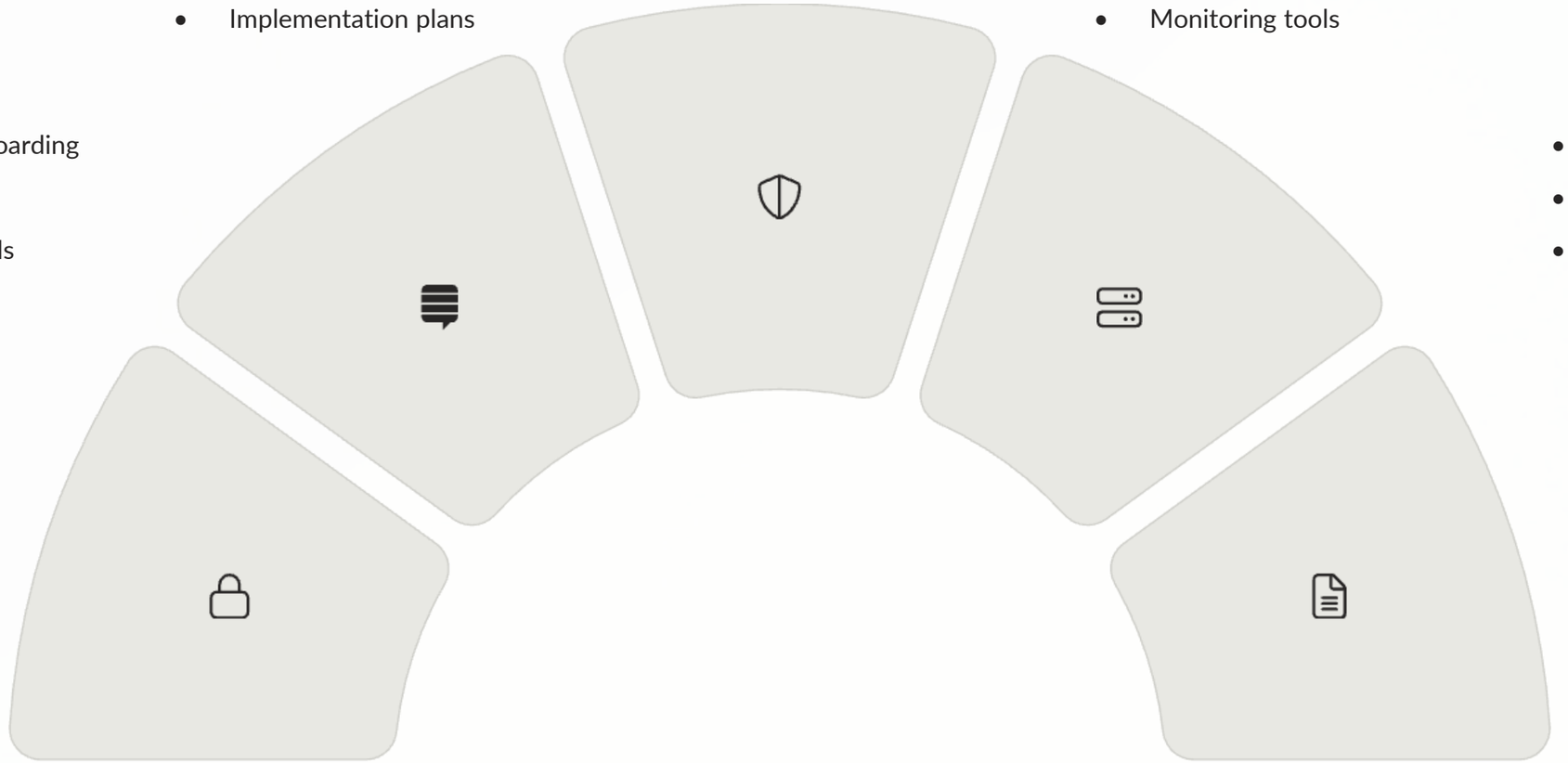
- System hardening
- Backup procedures
- Monitoring tools

Access Control

- User onboarding/offboarding
- Privilege reviews
- Authentication controls

Policies

- Security policies
- HR procedures
- Incident response



Evidence requirements vary based on your specific Trust Service Criteria, but these categories represent the core documentation needed for most SOC 2 audits. Work with your auditor to understand their specific expectations for format and detail level of each evidence type.

Managing Cross-Functional Collaboration

Regular Touchpoints

Schedule consistent weekly meetings with all stakeholders to review progress, address roadblocks, and maintain momentum. Include both technical and business teams to ensure comprehensive coverage.

Visible Progress Tracking

Create dashboards showing completion percentages by team and control area. Public visibility encourages accountability and highlights areas needing additional focus or resources.

Communication Channels

Establish dedicated Slack/Teams channels for real-time audit communication. Separate technical discussions from executive updates to maintain appropriate detail levels for different audiences.

Recognition Program

Combat audit fatigue by celebrating milestones and recognizing individual contributions. Consider small rewards for teams that consistently meet deadlines with high-quality evidence.

Preparing for Control Testing

Control Demonstrations

Prepare subject matter experts to walk auditors through control operations. Practice explanations that connect technical details to business objectives and security requirements.

Mock Audits

Conduct simulation exercises where team members role-play as auditors, asking challenging questions and requesting evidence. Identify and address knowledge gaps before the actual audit.

Evidence Validation

Verify that all collected evidence actually demonstrates the intended control objective. Have peers review evidence packages to identify incomplete or unclear documentation.

For Type 2 audits, focus on consistent control operation throughout the audit period. Help teams understand the importance of following documented procedures exactly as written, even for routine activities.

Understanding Type 1 vs Type 2 Audits

Type 1 Audit - Point-in-Time

Evaluates controls at a specific date

2

Type 2 Audit - Period of Time

Tests control operation over 6-12 months

Progressive Approach

Many organizations start with Type 1, then move to Type 2

The distinction between these audit types is crucial for project planning. Type 1 audits are simpler but provide less assurance to customers. They confirm controls are designed appropriately as of a specific date. Type 2 audits are more rigorous, demonstrating that controls operated effectively throughout the audit period.

For Type 2 audits, establish mechanisms to continuously collect evidence throughout the period. Missing evidence from earlier in the period cannot be recreated later.

Handling Exceptions and Gaps

24hrs

Response Time

Maximum time to acknowledge and begin addressing identified control gaps

72%

Prevention Rate

Control gaps caught through internal reviews rather than external audits

3-5

Documentation Updates

Average number of policy revisions needed during audit preparation

14days

Remediation Period

Target timeline for implementing missing controls before formal audit

Control exceptions are almost inevitable in complex environments. The key is how quickly and effectively you respond. Develop a standardized exception handling process that includes root cause analysis, immediate compensating controls, and permanent remediation plans.

Be transparent with auditors about known issues and your remediation approach. Most will appreciate proactive disclosure over discovering problems themselves.

Managing Pre-Audit Anxiety

Understand Auditor Mindset

Auditors are verifying controls, not trying to "catch" you. Their job is to provide a fair assessment, not to fail your organization. Approach the relationship as collaborative rather than adversarial.

Prepare Leadership

Brief executives on potential findings before they appear in reports. Set realistic expectations about the likelihood of exceptions, especially for first-time audits. Emphasize the improvement process.

Support Team Members

Recognize that team members may feel their work is being scrutinized. Provide talking points and coaching for those who will interact directly with auditors. Celebrate their preparation efforts.

Establish Escalation Paths

Create clear procedures for handling difficult audit questions or requests. Designate senior team members who can step in if discussions become challenging or technical details need clarification.

Post-Audit Activities

Review Draft Report

Carefully examine the draft audit report for factual accuracy. Provide feedback on any misunderstandings or mischaracterizations within the auditor's response timeframe.

Address Findings

Develop remediation plans for any control exceptions or observations. Assign owners and deadlines for each finding to ensure timely resolution.

Conduct Retrospective

Facilitate lessons learned sessions to identify process improvements for future audits. Document what worked well and what needs adjustment.

Build Continuous Compliance

Integrate control monitoring into regular operations. Establish quarterly internal reviews to maintain compliance between formal audits.

The end of the audit is the beginning of your continuous compliance journey. Use the experience and feedback to strengthen your control environment and streamline future audit processes.

Keys to SOC Audit Success

Start Early

Begin preparation 6-12 months before your target audit date

Engage Stakeholders

Secure cross-functional buy-in and active participation

Improve Continuously

Use each audit cycle to strengthen your security posture

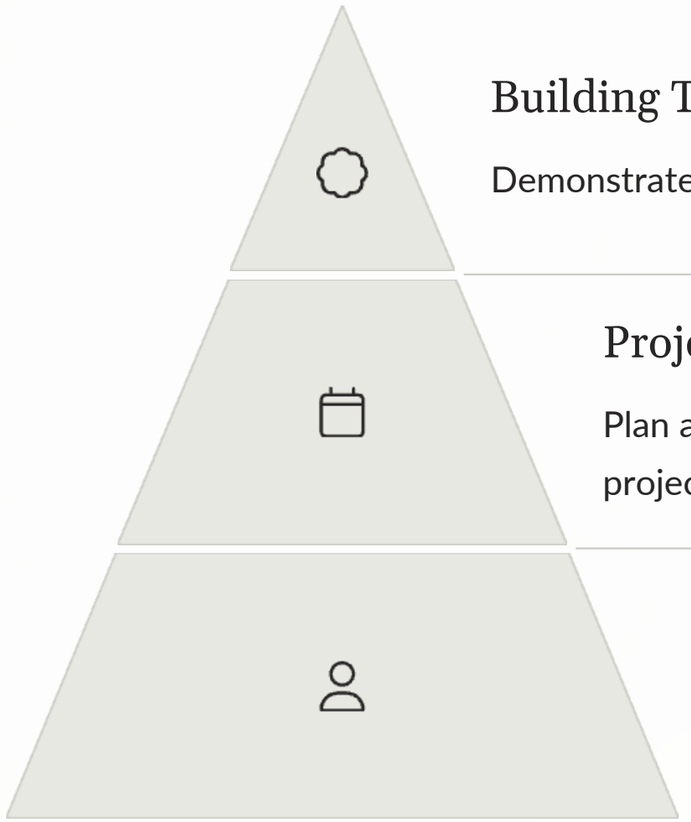
Document Thoroughly

Maintain clear, consistent evidence throughout the audit period

A successful SOC audit requires careful planning, cross-functional collaboration, and attention to detail. As project managers, we serve as the vital connective tissue that brings these elements together.

Remember that compliance is a journey, not a destination. Each audit cycle should build upon the previous one, creating a culture of continuous security improvement within your organization.

Final Thoughts



Building Trust

Demonstrates commitment to protecting data

Project Management

Plan ahead and manage like any critical project

Team Engagement

You're the glue that keeps the process moving

A successful SOC audit is more than just a security badge—it's about demonstrating your organization's commitment to protecting customer data and building trust. As a project manager, you play the crucial role of keeping this complex process on track.