SOC Toolkit Guide

Understanding the Toolkit

What is this toolkit and how should I use it?
The toolkit helps summarize the entire SOC (Service Organization Control) report and distinguish which controls are covered, adequately tested, and can be relied upon to reduce testing in a certain audit area.

Is this toolkit a replacement for the full SOC report?
No, the full SOC report must still be obtained and verified as applicable to your audit. The toolkit is a resource to be used in conjunction with the SOC report.

Who typically uses this toolkit?
The toolkit is typically utilized by audit firms to gain an understanding of the organization and the operating effectiveness of the controls listed.

When should I request the SOC report from the service provider and the corresponding toolkit from AuditMiner?
The SOC report should be requested during the planning stage when accessing the audit package, with the toolkit obtained immediately afterward. Reviewing the SOC report early is essential, as it provides a deeper understanding of the organization and applicable controls. The report may highlight exceptions or qualifications that may affect planned audit approach.

Are AuditMiner SOC Toolkits regarded as specialist work?
No. AuditMiner SOC Toolkits offer firms a streamlined and consistent approach to reviewing and documenting SOC reports. While they significantly enhance efficiency and standardization in audit workflows, it is important to clarify that these services do not constitute the use of a specialist under AU-C Section 620. Refer to our Resource Library for additional information: https://help.auditminer.com/using-soc-toolkits-in-audits.

Scope & Content of SOC Reports

What time period does the SOC report cover?
Periods vary, but to evidence operating effectiveness, the report must cover six months or more of the audit year. If shorter, an additional report or a bridge/gap letter is needed. For instance, if SOC report covers through 9/30/XX, but the audit period ends 12/31/XX, a bridge/gap letter can be obtained to cover the period from 10/1/XX to 12/31/XX. Bridge/gap letters are treated similar to a Type 1 report, as no tests of controls took place to verify operating effectiveness.

Which services and systems are included in this review?
The opinion page lists the service under audit. Subservice organizations, if used, are also identified along with any carve-outs.

What are Carve-Outs and why are they important?
Carve-outs are subservice organizations' controls that are excluded in the main service auditor's report. These can range from IT and recordkeeping services, which are significant to the audit, to minor services like printing. When evaluating a carve-out, the key question is whether anyone has access to the data or system; if so, the subservice organization's report must be obtained and assessed. Evaluations are audit-specific, so AuditMiner provides only general recommendations.

How are carve-outs determined, and why are some required while others are not?
It depends on the type of carve-out:

- Custodian/Trustee: Not required, as certifications cover investments.
- ITGC controls: Usually required to ensure adequate coverage.
- Recordkeeper: Typically required for all EBP audits.

From there, auditors assess whether the subservice organization had access to or could manipulate data undetected.

What are Complementary User Entity Controls (CUECs)?
These are controls at the user organization that must be in place for the service organization's controls to operate effectively. They are a key part of the overall risk assessment process. They should be integrated with the relevant audit procedures and walkthroughs.

How should I evaluate direct vs. indirect controls when reviewing a SOC report?
SAS 145 requires auditors to distinguish between direct controls that address financial reporting risks and indirect controls, such as IT general controls that support the direct controls. The toolkit highlights these areas, but auditors must determine if direct control coverage is sufficient. If only indirect controls are present, additional procedures may be required.

Using the Toolkit in an Audit

How do I integrate this toolkit into my audit process?
The toolkit provides a summary of the SOC report and should be added to the audit file alongside the full report. It helps identify any additional reports needed, determines which controls are sufficient to reduce testing, and highlights which CUECs must be completed to use the SOC report effectively.

What should I do if I identify exceptions in the controls?
Exceptions should be evaluated individually, and additional procedures may be required. While the service auditor typically performs additional testing, it is not guaranteed. Additional procedures might include identifying mitigating controls in the report, relying on a Plan Sponsor control, performing another walkthrough, or opting for non-reliance. Management responses to exceptions can provide useful guidance and serve as a starting point on how to address the risk.

When should complementary user entity controls (CUECs) be marked as not relevant?
Mark CUECs as not relevant when the control objectives (COs) they apply to are not relevant.

How should I complete the "Test of Controls" box if I do not test controls, do not plan to rely on the SOC report, or reduce sample size?
In the CUECs tab, select "No" under Reducing Control Risk then leave the rest of the box blank. In the Conclusion tab, indicate "No reliance taken" and delete testing areas listed under "The controls identified above will be relied upon…". Keep in mind, the CUEC walkthroughs must still be completed to verify operating effectiveness of the controls in order to properly conduct the SOC review.

If a walk-through procedure on the CUEC tab is not applicable, can I edit it?
Yes. The walkthroughs on the CUEC tab are suggestions and should be modified as appropriate. Similarly, the carve-out tab may also be adjusted at the auditor's discretion, based on the plan under audit, the plan sponsor controls, and firm-specific practices.

In a full-scope audit, do all the controls still apply?
These toolkits are geared towards limited scope audits. If you have a full-scope audit, then some of the controls objectives marked "No" may apply. These are not reflected in the Conclusion tab.

Why are controls marked as "Yes" on the CO page but not shown on the Conclusion page?

Always review the Notes column on the CO page. There are several possible reasons:

- Key controls needed for reliance may be missing.
- The control may be listed but not adequately tested.
- Testing may have been limited to inquiry and observation only.
- Tests may not have gone down to the participant level.

In most cases, the rationale will be documented in the Notes column.

When the opinion is qualified, what additional steps are required?

It depends on the nature of the qualification. We address the impact when it affects relevant control objectives, but specific steps vary by firm and engagement. Each audit firm is responsible for reviewing qualifications and determining their effect on the audit.

Understanding Key Terms

What do the control objectives (COs) mean?

The service organization provides a summary of their processes and how they conduct business. The service auditor walks through these processes and identifies the controls that are present. Audit firms, as user organizations, assess whether there is sufficient evidence to support risk assessment and verify control design and implementation (typically in Type 1 and Type 2 reports). The next step is evaluating evidence of operating effectiveness through the service auditor's control testing, which is only included in Type 2 reports.

What does "Type 1" vs. "Type 2" report mean?

Type 1: Describes the system and control design at a point in time. No testing is performed.

Type 2: Includes testing of controls over a period, providing assurance on operating effectiveness.

What is the difference between a SOC 1, SOC 2, and SOC 3 report?

SOC 1: Covers financial assertions (used in EBP audits).

SOC 2: Focuses on IT and critical systems controls.

SOC 3: Similar to SOC 2 but less detailed, intended for general use.

Limitations & Clarifications

How are toolkits typically named?
Toolkit names follow the naming convention used by the service organization auditor for the entity under audit.

Does this toolkit include every detail from the SOC report?
No, it is a summary of key points.

Can I rely solely on the toolkit for compliance purposes?
No, the SOC report must be included in the audit workpapers. The toolkit should be used in conjunction with the actual report.

How does scalability under SAS 145 affect the use of this toolkit?
SAS 145 requires audit procedures to scale with entity size, complexity, and risk. The toolkit supports this by offering a framework that can be expanded for complex audits or streamlined for simpler ones while maintaining compliance.

Who can I contact if I have questions about the toolkit?
Email us at support@auditminer.com