R-VMC

Re-Vision Management Consulting

SOC Compliance Steps and Recommendations

The primary first step is understanding what your customer(s) want regarding a "SOC" report. SOC 1, 2, or 3? Type 1 or Type 2? A one-time report or ongoing (year to year)? Once you understand what they want, you'll have a better roadmap to success.

Before a SOC Audit:

You'll want basic "internal controls" in place which mirror standard SOC controls.

Examples include:

- Daily backups of critical servers
- Restricted user access rights regarding customer data
- New hire checklists
- Termination checklists
- Helpdesk ticket system
- Policies such as employee handbooks, confidentiality agreements, and system changes

Once you feel like "standard" controls are in place, you'll want to select your SOC audit firm. The larger the firm, the more expensive it will be.

The firm will complete a "readiness assessment", which is essentially a "this is the current status of your controls and what you need to fix/implement".

You will then agree on the start date of your audit period (typically 1-2 months after the assessment). The gap between the assessment and the start date is when you must address all issues in their report.

During the SOC audit period

Important factors to note during the period:

- All controls must be in place during the ***entire*** audit period.
- You'll want to ensure all audit evidence is kept in an orderly manner to help the audit go smoothly
- Changing of personnel, changing of processes, changing systems or applications are not excuses for any controls not being in place

The SOC Audit

Typically, an audit firm sends its initial request list about a month before on-site work. They complete walk-throughs with each "control owner" and request samples for every control. Initial population requests (i.e. a report of all new hires for the audit period) are given two weeks to provide, then another 1-2 weeks to provide request sample support.

If a sample of 25 new hires is selected and you can't provide the new hire checklist for one of the samples, every control which relies on the checklist will fail the audit.

Post-Audit

Your new audit period typically starts the day after your previous audit period. This means all controls implemented during the pre-audit phase are now part of your standard, daily, procedures.

The SOC report is typically issued to you 45-60 days after fieldwork. No surprises should be on the report if the audit firm has done its job correctly.

How R-VMC can help.

Pre-Audit support

- We know most of the controls you'll need to implement, we can train and guide your team through the implementation process
- We can help create policies and procedures required for compliance
- We have great relationships with audit firms who specialize in SOC, we can recommend the right firm for your organization (we have no monetary influence on this recommendation)
- We can work with your team post-readiness assessment to help implement controls before the audit period
- We can negotiate with your auditors regarding control wording, frequency, and other critical details

During the audit period

- We help complete some controls (IT security training and annual risk assessment are two common ways we support our clients)
- We conduct practice audits and training to help ensure controls are properly in place and audit evidence will pass the auditor's review

During the audit

- The longer you take to reply to auditor requests, the more annoyed they become and the more critical they are of your controls. We manage the audit, being the direct contact for the audit requests and questions, ensuring timely AND accurate support is submitted.
  - *This reduces the stress and time put on your team during the audit and keeps your auditors happy*

Contact us at Thomas@r-vmc.com to learn more about how we can support you and your team through the SOC process.