On the Road to SOC 2 Readiness

What Service Organizations Need to Know
Successful organizations know the importance of focusing on core competencies. This understanding, coupled with advancements in the quality and capabilities of procured services, are driving a trend toward replacing in-house IT applications, systems and related processes with third-party services. Such services are popular for their enhanced capabilities, operational simplicity and lower cost. Entrusting confidential customer information, trade secrets and employee data to outside parties, however, has made it important for organizations to demonstrate — for customers and regulators — that data and systems are well-controlled and available, regardless of where the data resides.

Although responsibility for managing IT risk will always reside within the organization, the burden of assuring that appropriate controls are in place for outsourced processes and systems is being pushed down to the service provider.

From this focus on the service organization’s environment has come a groundswell of security and control questionnaires and vendor audits. These efforts are not only time-consuming, but often come with results that are lacking in consistency and substance. Stakeholders on all sides of the issue have sought ways to provide proactive assurance and reduce ad hoc compliance requests. For many, the Service Organization Control report (SOC 2), issued by a service auditor, has become the assurance standard of choice — to the point that many organizations now contractually require vendors to provide annual SOC 2 reports.
What is SOC 2?

In 2011, the American Institute of Certified Public Accountants (AICPA) created a series of Service Organization Control (SOC) assessments. 1 The assessment reports require a controls audit to be performed by a CPA firm (also known as a service auditor) and provide different levels of assurance and detail depending on the type of SOC report. This includes financial controls assurance (SOC 1, previously SAS 70) and controls assurance over operational elements of a service organization’s environment (SOC 2 and 3). A SOC 2 report includes details of the test results, controls and specific tests performed, whereas the SOC 3 report covers a similar scope, but only provides a summary of the systems audited and the results of the assessment, with no details of the control environment. SOC 1 and SOC 2 reports can be issued as a Type I or Type II — Type I providing an assessment of the design of the controls, and Type II providing the design assessment, as well as an audit of operating effectiveness using industry standard control techniques.

A SOC 2 is an attestation report that provides controls assurance over a defined set of the service provider’s systems. Each report covers a defined period of time (usually nine months) to be agreed on between the service auditor and service provider. The report can encompass between one and five trust services principles (TSP), depending on the needs of the service organization, which include: security, availability, processing integrity, confidentiality and privacy.

The security principle is one of the most commonly selected and is used to determine whether relevant systems are protected against unauthorized access, use or modification.

Deciding to obtain a SOC 2 report is not a one-time event; it requires an ongoing commitment — a commitment from management that controls will be performed consistently, and a financial commitment to hire a service auditor to perform testing over several months and issue a report annually. With that commitment often comes the realization that an organization’s culture needs to shift toward a more formal framework of controls and testing, to help ensure favorable audit results (known as an unqualified opinion) and satisfied customers. Consistent execution of the controls is critical and often requires significant remediation before an organization is ready to submit to the service auditor’s testing.

Most service organizations have yet to develop the control frameworks and tools required to meet the rigorous SOC 2 audit standards. Given the critical importance of a positive report, and the potential reputational and economic consequences of a negative one, service organizations are turning to outside consultants to help them prepare by identifying gaps against the SOC 2 standard, conducting a readiness audit, and remediating controls and processes that would not pass muster.

Preparing for SOC 2

Getting ready for an initial SOC 2 audit can be arduous and time-consuming, depending on the scope and level of complexity in the environment. The process begins with developing an understanding of what is driving the need for a SOC 2 audit and the systems that are relevant to those drivers. It continues through a gap assessment and an iterative cycle of remediation and readiness testing, correcting control and design gaps along the way, until results fall consistently within an acceptable range of outcomes, as outlined below:
**Scope**

The scope of a SOC 2 report depends on the type of service a vendor provides, as well as the needs of its customer base. A thorough scoping should seek to determine which TSP(s) customers will require assurance with, and which systems and components must be assessed to do that. A service organization can select any number and combination of the TSPs for inclusion in the report, based on customer need and relevant contractual requirements.

In some cases, organizations may deem two or more TSPs to be relevant to their customers’ needs. In our experience, and depending on a number of factors, including existing process maturity and culture, it is sometimes best to follow a staged approach to addressing multiple TSPs, focusing on the most important TSP first and increasing the scope of the report in the future. Organizations that attempt to address multiple TSPs as part of their first SOC 2 project increase the risk of disruption to normal operations, missed target dates and, potentially, a qualified initial report. Service organizations should work with their advisers to determine the best approach that fits the needs of their customers, as well as their own organization.

The five TSPs include:

1. **Security**
   The system is protected against unauthorized access (both physical and logical).

2. **Availability**
   The system is available for operation and use as committed or agreed.

3. **Processing Integrity**
   System processing is complete, accurate, timely and authorized.

4. **Confidentiality**
   Information that is designated “confidential” is protected as committed or agreed.

5. **Privacy**
   Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity’s privacy notice and with the criteria set forth in generally accepted privacy principles.
Ultimately, the system scope of a SOC 2 assessment is at the discretion of management and will be clearly described within the SOC 2 report. As such, if the scoping exercise does not draw the system boundaries appropriately, customers may not be satisfied with the SOC 2 report and may request additional information, or even a separate audit — limiting the value of the exercise. Getting the scope phase right is critical to the success of the SOC 2 process.

**Assessment**

After the scope has been determined, the next step is to evaluate management’s control environment using the SOC 2 criteria customized to the chosen TSPs to identify gaps requiring remediation.

<table>
<thead>
<tr>
<th>Trust Services Principle</th>
<th>SOC 2 System Scoping Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>“Would compromise of this system threaten the security of our customers’ data or IT environments?”</td>
</tr>
<tr>
<td>Availability</td>
<td>“Is this system important to ensuring continuity of service to our customer?”</td>
</tr>
<tr>
<td>Processing Integrity</td>
<td>“Would a breakdown of control in this system result in lack of integrity in customer data?”</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>“Does this system house, transmit or otherwise protect customer data classified as confidential?”</td>
</tr>
<tr>
<td>Privacy</td>
<td>“Does this system house, transmit or otherwise protect customer personal data?”</td>
</tr>
</tbody>
</table>

The assessment process can be broken out into the following high-level steps:

- Mapping of existing controls to the framework
- Documentation of gaps and “future state” controls
- Identification of remediation plans

The mapping process should start with a review of control documentation that may already exist, relevant to the scope and the control objectives identified in the SOC 2 standard. This could include sources such as Sarbanes-Oxley Section 404 compliance, internal audit, risk management, control self-assessments, past advisory assessments, or policies and procedures.
Walk-throughs of management’s existing processes will provide a more complete view of the relevant processes and controls, and will provide the SOC 2 team with most of the information it needs to understand where management’s controls align to the standard and where gaps exist. It is critical to involve the correct stakeholders and process owners in these conversations to ensure the accuracy of the information. Inaccurate control information can lead to delays later on, or if not identified early enough, testing exceptions in the SOC 2 audit.

Mapping of processes and identification of gaps is a highly collaborative process, as there is no single correct approach to addressing the requirements of the SOC 2 standard. It is important to involve a knowledgeable, experienced IT risk and control team in the process, as the service auditor will likely take a very detailed approach to reviewing the final set of controls to ensure that SOC 2 objectives are met. While the specific technologies, processes and organizational roles established as part of the control environment are up to the discretion of management, achieving an appropriate level of control in light of the service provider’s organizational size and complexity, data risk profile, volume of customer activity, and other related factors is critical.

Remediation

Remediation plans should serve as a detailed road map toward the execution of a SOC 2 report. For every gap in the control environment, a remediation plan that includes the following elements should be articulated:

1. Detailed steps and deliverables to satisfy the control standard
2. Timelines that are feasible, yet aggressive in meeting goals
3. Remediation owners to track and motivate progress

There should be periodic meetings for all those involved in SOC 2 remediation activities or processes. Considering that many TSPs affect the service provider as a whole, and not just the IT department, it is critical to gather all relevant parties and solicit their input on remediation feasibility and process improvements. In addition to addressing the specific matters at hand, these meetings can serve to foster a culture of SOC 2 compliance, which is imperative, especially for organizations completing the assessment for the first time.

Some gaps are easily remedied. Others will require a more significant time and cost investment, as well as changes to established systems, processes, cultures and subject-matter expertise.

While organizations will always have an initial target date in mind for SOC 2 readiness, the results of the gap analysis and extent of remediation plans will dictate the feasibility of those initial targets. Depending on the drivers for the SOC 2 assessment and the importance of meeting its target date, management may need to augment its capabilities temporarily with the help of an outside adviser in order to implement the necessary control enhancements within a designated time frame. Alternatively, the timeline may be extended in order to achieve remediation with a smaller complement of resources, should remediation plans call for this. The most important goals for management coming out of the remediation phase should be to maximize repeatability of processes and to achieve a stable, consistent control environment that addresses SOC 2 requirements.

Readiness Testing

No matter how ready a service organization may appear on paper, it is important to conduct readiness testing to ensure the organization’s controls work as intended. This should be done before engaging a service auditor. Readiness testing reduces the risk of
exceptions that could result in qualified opinions and serves to validate management’s assertions made during the documentation and remediation phases. Even when remediation appears to be complete, experience has shown that testing will uncover human error. Controls that were not flagged as gaps during the assessment phase, and in which management has significant confidence, can often be shown to operate ineffectively through control testing. Only when an organization has submitted to readiness testing and addresses its operating effectiveness issues should management feel confident to move forward with its first SOC 2 audit.

Conclusion

With the absence of a structured readiness approach, there is a risk of failure. Engaging a public accounting firm to conduct the SOC 2 assessment and then releasing a report with multiple control failures, the service organization risks distributing a report with failures that could have brand impact or create compliance issues for customers, or delaying the SOC 2 report that may be contractually required by critical business partners. Obtaining a SOC 2 report can be an ideal solution for many service providers looking for a more efficient way to satisfy customer inquiries about their control environment, but a structured readiness process is critical. SOC 2 readiness requires perspective from experienced IT risk and control professionals to make the right judgment about the level of control that will satisfy the AICPA standard and result in an unqualified report. More than just an IT exercise, SOC 2 readiness should be viewed as a companywide opportunity for service providers to gain competitive advantage through risk management maturity. Taking a methodical approach to identifying controls that align to the standard, remediating the gaps, and validating control effectiveness will help service providers achieve SOC 2 readiness and confidently face the future.
ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

HOW PROTIVITI HELPS CLIENTS FACE FUTURE UNCERTAINTY CONFIDENTLY

As a professional services firm with deep expertise in IT, risk and control, Protiviti is uniquely positioned to assist service organizations with readiness and the remediation of SOC 2 control gaps. We serve as an extension of management, working with prominent accounting firms to understand their audit and control testing requirements.

In addition to documenting controls, advising on remediation and performing control testing and validation, we assist clients with readiness project management. Through our parent company, Robert Half, an industry leader in staffing services across a variety of domains, we can also provide supplemental staff where required.

CONTACTS

Gordon Braun  
+1.913.661.7406  
gordon.braun@protiviti.com

David Lehmann  
+1.212.708.6370  
david.lehmann@protiviti.com

Noah Kessler  
+1.646.428.8211  
noah.kessler@protiviti.com