SOC 2+®: An integrated and proactive approach to attestation

November 2016

kpmg.com

SOC 2+®: An integrated and proactive approach to attestation

Organizations are growing increasingly sensitive to the potential financial and reputational risks associated with using service providers. Now, more than ever, customers, regulators, and business partners want to know that their data is being properly protected by their service providers.

The need for such knowledge about data security has placed a growing burden on the service providers themselves, and many are now investing significant time and resources towards responding to the various independent attestation requests they receive from their customers.

However, with SOC 2+® reporting, service providers can now take a more efficient approach that can deliver improved customer confidence and potentially reduce costs.

A growing burden of customer needs and requests

For service providers—essentially any business or organization that handles third-party data—attestation reporting remains an undeniable part of doing business.

The vast majority of service providers have been beholden to the Service Organization Controls 2 (SOC 2®) reporting framework for nearly five years.

The problem is that—while the SOC 2® framework was intended to meet the needs of a broad range of users—many customers continue to request different reports (and often send in their own audit teams) to review elements that may not be included in the traditional SOC 2® framework. And that is creating additional work for both the service providers and their customers.

The reality is that SOC 2® was developed to provide assurance on service providers' controls related to security, availability, confidentiality, processing integrity, and privacy. Due to the diversification of the customer base, the needs of such customers have grown to include reporting on controls related to additional areas.

For some service providers, such additional controls relate to the business sectors of their customers or the types of information transmitted by such customers. For example, banks operate in a very different environment than healthcare providers in that they transmit different types of information and are subject to different regulatory requirements. For others, the additional controls relate to the specific customer type (public sector versus private sector). Additionally, there are regulations from a multitude of foreign jurisdictions that may apply to a specific service provider or customer, which fuels the need for additional coverage.

Beyond SOC 2®

Service providers may be required to report against multiple control frameworks above and beyond SOC 2®. These may include:

- The International Organization for Standardization (**ISO**) **27001**
- Cloud Security Alliance's (**CSA**) Cloud Controls Matrix (**CCM**)
- Health Information Trust Alliance's (**HITRUST**) **CSF**
- Control Objectives for Information and Related Technology (**COBIT**) **5**
- Committee of Sponsoring Organizations of the Treadway Commission (**COSO**) **2013**
- National Institute of Standards and Technology (**NIST**) **800-53 R**
- Health Insurance Portability and Accountability Act (**HIPAA**)
- Federal Information Security Management Act (**FISMA**)

Looking for a better way

Not surprisingly, many service providers have put significant time and resources towards reacting to meet individual customer requirements. The more sophisticated service providers undergo annual certification against multiple risk and control frameworks in order to reduce their attestation burden, while others are left struggling to meet the demands of their customers through antiquated and often costly means.

More recently, however, some service providers have started to question whether there is a better way. We believe there is—SOC 2+®.

In contrast to a traditional SOC 2® report, SOC 2+® reports incorporate independent auditor's opinions on **additional criteria or subject matter.** The ability to include additional criteria or subject matter enables the service provider to incorporate customer requests into an established reporting framework, often expanding on an existing report to increase efficiency and customer satisfaction.

Some examples of additional subject matter include adherence to a statement of a third-party's privacy practices, adherence to Service Level Agreement (SLA) requirements, and physical control attributes (such as data center cage locks) at a service organization's facility. Examples of additional criteria include NIST 800-53 and HITRUST.

Putting the "plus" into SOC 2+®

SOC 2+® is an enhanced reporting option that allows the service organization to demonstrate controls that meet the Trust Services Principles and Criteria (TSPs) and additional criteria or subject matter. While the SOC 2+® increases the criteria covered, there may be significant overlap between the TSPs and the selected additional criteria, which allows service providers to realize efficiencies in reporting.

At KPMG, we have developed a proprietary tool called Control Framework Integration Tool, or CFIT that allows our professionals to look across frameworks and map the overlapping controls. CFIT supports standards and frameworks such as SOC 1, SOC 2®, NIST 800-53, NIST Cybersecurity, Federal Information System Controls Audit Manual (FISCAM), ISO 27001, Federal Risk and Authorization Management Program (FedRAMP), and the HITRUST CSF (and we are continuously investing in the implementation of additional standards and frameworks to add to the list). This means that we are better prepared to help organizations identify the overlapping controls, gain efficiencies, and minimize costs.

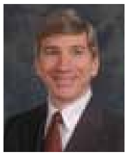
We recently worked with a U.S.-based data center and hosting provider that serves customers across a variety of industries. They needed to provide a SOC 2® to their customers and also demonstrate controls related to additional criteria, specifically NIST 800- 53 rev. 4. By identifying and testing the relevant set of controls once, we were able to develop attestation reports that the data center provider could share with their customers. This led to significant savings of over 30%* in the service provider's cost of demonstrating controls in alignment with NIST 800-53 rev. 4. It also allowed the organization to create a consistent approach for including additional criteria (such as HIPAA and FISMA) in the future.

*Each service provider's actual savings are based on individual circumstances.

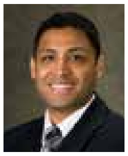
We believe that it is time for service providers to take advantage of the synergies of overlapping control frameworks and satisfy their customers' evolving control requirements. This answer starts with a SOC 2+®.

Contact us

For more information on KPMG's Risk Consulting Services related to SOC 2+®, please contact:



Chris Mottram
Partner
Advisory Services
T: 404-979-2100
E: cmottram@kpmg.com



Sai Gadia
Managing Director
Advisory Services
T: 612-305-5087
E: sgadia@kpmg.com

Emily Frolick
Partner
Advisory Services
T: 513-763-2453
E: efrolick@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.