OUM&CO™
ACCOUNTANTS & BUSINESS ADVISORS

Evolution of SOC 2 Reporting

The American Institute of Certified Public Accountants (AICPA) has released a new SOC 2 guide (AICPA Guide SOC 2 Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy). The guide supersedes the 2016 edition of the Trust Services Principles and Criteria for reports with period ending dates on or after December 15, 2018, with early adoption permitted.

Why the change?

With the rapid use of technology, the compliance requirements for various industries have continued to evolve over the past couple of years. Outsource Service Providers (OSPs) are in huge demand as they help organization focus on their core business and transfer less critical business operations to them. With the changing business model and this transfer of responsibilities there is a huge emphasis on OSP's internal control structure and cyber risk management programs.

On May 14, 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its updated 2013 Internal Control-Integrated Framework. The 2013 framework was updated to address significant changes in businesses, which have become more complex and technology-driven. The key focus of the COSO framework was to provide working guidance over monitoring outsource service providers, reflecting the business model changes and increased relevance of technology.

The COSO 2013 framework, and associated guidance for organizations to provide oversight and monitoring over OSPs, has matured over the years which has been adopted by AICPA while formalizing the Trust Services Criteria's for SOC 2 reporting.

What to expect with the new Guidance?

1. Verbiage changes–There are few verbiage changes, wherein the trust services principles and criteria are now referred to as the trust services criteria (TSC), and the principles are now referred to as the trust services categories. Point of focus are added for each TSC which aligns with COSO2013 framework and provides a guiding hand for achieving each TSC. The Information security requirements have been organized logically and grouped as below:

- Logical and physical access controls
- System operations
- Change management
- The trust services criteria also address risk management, incident management, and certain other areas at a more detailed level than in the past.

2. Incident management and disclosure–The guide recommends disclosure of incidents, including but not limited to Cyber Incidents. The criteria also include helpful guidance related to disclosures, including what to consider when determining whether to disclose an incident or no. The disclosure does not necessary require to consist of all security details but enough for the reader of the report to understand the risks at the service organization and its impact.

3. Formal alignment to SSAE18 standard–There is an effort to include various elements of the SSAE18 standard published in 2017 within SOC2 reporting:

- Risk Assessment
- Inclusion of Complementary Sub Service organization controls
- Evaluating the reliability of information produced by the service organization
- Identifying complementary subservice organization controls
- Clarification of complementary user entity control considerations

CONTACT

Chris Millias
Partner: Assurance & Advisory
cmillias@oumcpa.com
415-796-6530

Doug Pallotta
Partner: Assurance & Advisory
dpallotta@oumcpa.com
415-796-6570

Darwin Pangilinan
Partner: Assurance & Advisory
dpangilinan@oumcpa.com
415-796-6570

Mustafa Kagalwala
IT Advisory Director
mkagalwala@oumcpa.com
415-796-6703

OUM&CO™
ACCOUNTANTS & BUSINESS ADVISORS

San Francisco-Main Office
601 California St.
18th Floor
San Fransisco, CA 94108
415-434-3744

San Diego Office
1917 Palomar Wy #100
Carlsbad, CA 92008
800-208-3367

Visit our website at oumcpa.com