The new SOC 2 privacy principle guidelines:
What do you need to know?

pwc

Do you have customers that plan to audit you? Are customers asking about privacy? The SOC 2 privacy criteria are changing – and here's what you need to know.

Service organisations are signing more contracts requiring them to issue a Service Organisation Control (SOC) 2 report and many of these contracts require that all five of the Trust Services Principles – security, availability, processing integrity, confidentiality, and privacy – are covered. For many, getting a firm grasp on all of the principles, particularly on privacy, has proven difficult. As the privacy requirements are currently written, the criteria can be tough to understand, redundant, and sometimes impractical. As a result, many service organisations have avoided the privacy SOC 2 principle and, in turn, struggle to meet contract terms that stipulate their operations must be assessed against the Trust Services Principles.

Help is on its way

In June 2015, the Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accountants (AICPA) released an exposure draft that, among other aspects, includes an updated version of the trust services criteria for privacy. This update was specifically undertaken to eliminate redundancy and ultimately clarify the requirements of this principle. With the revised criteria set to be published in the summer of 2016, ASEC aims to make all the trust services criteria – including those for privacy – more user friendly and easy to manage.
For companies holding off on issuing reports that include the privacy principle, they need not wait any longer.

Establish your SOC 2 plan

Though it may seem intimidating, many service organisations are beginning to cover all five trust principles in their SOC 2 reports. These organisations are first going through "readiness" in order to ensure they have the right policies, processes, and controls in place to comply with all five trust principles. Performing these readiness engagements and methodically addressing each trust principle, including privacy, is allowing both companies and their vendors to have increased transparency and trust with each other.

In our experience, very few organisations can "pass" a SOC 2 examination without some type of remediation, whether it's adding new controls or retaining documentation that would not otherwise have been retained.

Regardless of your state of affairs, you'll want to gather knowledge on several critical questions:

- Do you need to address all five principles or just one or two?
- Which trust principles are appropriate for your business model and for the relationships you have with your vendors?
- Do you need to issue a Type I or Type II report?
- What is the appropriate scope for your SOC 2 reports?
- Do you need to test all systems or just a few?

For those service organisations that have not yet been asked for a SOC 2 report, chances are the request is on the way. The next front page news story about an outage or data breach will quickly move a SOC 2 report from a "nice to have" to a "must have" on your customers' risk assessment checklists.

What are the proposed changes?

The purpose of the exposure draft is to revise the criteria related to privacy by deleting the criteria that are already addressed by the common criteria, and revising the remaining privacy criteria to create additional privacy criteria.

The following summarises what ASEC believes would be the most significant changes to the existing Trust Services Principles and criteria:

New set of Privacy criteria	The Generally Accepted Privacy Principle (GAPP) will be superseded by the common criteria and the additional criteria for the privacy principle.
Adds illustrative risks and controls related to privacy	The Illustrative Risks and Controls have been revised to include the additional privacy criteria and examples of risks that may prevent the privacy criteria from being met as well as controls designed to address those risks.
Adds clarifications	The criteria were modified to clarify that the potential threats include those arising from the use of vendors and other third parties providing goods and services as well as threats arising from customer personnel and those with access to the system.
New confidentiality criteria added	Two additional confidentiality criteria were added, to address the retention and disposal of confidential information.

The privacy criteria will now be organised in eight categories.

1. Notice
2. Choice and consent
3. Collection
4. Use and disposal
5. Access
6. Disclosure and notifications
7. Quality
8. Monitoring and enforcement

PwC however considers that additional guidance on when the privacy trust principle has been met, particularly when the nature of the entity's business model is such that certain of the eight categories related specifically to privacy are not applicable (as communicated to the AICPA in comment letter to the Exposure Draft dated 14 September 2015).

Demand for SOC 2 reporting is higher than ever and organisations should consider getting ahead of the game by thinking about how ready they are to withstand the rigors of the audit. Working with an experienced professional can help organisations navigate through this complex process and gain a competitive advantage by providing greater transparency to their customers.

Contacts

PwC offers a broad range of service organisation controls reports. In addition to providing SOC 2 solutions to our clients, we also develop and deliver customised attestations so you can approach both existing and prospective customers with confidence – and vigorously convey the trust and transparency that those customers need and expect. By bringing together industry-specific skills in technology, regulatory compliance, financial and accounting operations, and other business processes, PwC can help you assess your third-party risk management programme, with a focus on controlling costs, mitigating risk, and enhancing trust and transparency.

To have a deeper discussion on SOC reporting and the Trust Services Principles, please contact:

Nick Hamer

Third Party Trust China and Hong Kong Leader
+852 2289 8545
nick.j.hamer@hk.pwc.com

Aileen Wang

Partner, Shanghai
+86 (21) 2323 6655
aileen.wang@cn.pwc.com

Albert Lam

Partner, Beijing
+86 (10) 6533 7923
albert.t.lam@cn.pwc.com

www.pwchk.com