Successful companies constantly search for opportunities to strengthen the bottom line by focusing on their core businesses.

One approach is to outsource back office activities to third party service providers who can operate, collect, process, transmit, store, organize, maintain, and dispose of business information for user organizations.

Examples of outsourced functions include cloud computing, hosted data processing, payroll, and invoice processing. Properly managed, companies outsourcing support activities can add specialized skills to their business thereby gaining a competitive advantage.

However, outsourcing is not without risks. With outsourcing, a user entity exposes itself to additional risks related to the service organization's system. These risks include business, technology, governance/vendor management, and information leakage. The following are examples of such risks:

- Data security over public networks
- Service organization insider risks
- Data privacy
- Vendor ‘lock-in’ impairing the ability to change service providers
- Data loss and leakage

To assess and address risks associated with the outsourced service, management needs information about controls over the service organization’s system that affect the services provided to the user entity. The limit on the transparency into a service organization’s control environment underscores the importance that an activity can be outsourced, but not the responsibility for controls over how that activity impacts the security, privacy and continuity of business data.
Informed Trust

The AICPA helps clients and their auditors gain third-party assurance through reports such as Agreed Upon Procedures (AUP), Trust Services (Systrust), or those based on Statement on Standards for Attestation Engagements (SSAE) No. 16, formerly known as Statement on Auditing Standard (SAS) No. 70*. While there are other reports on processing activities, such as those based on Payment Card Industry (PCI) or International Organization for Standardization (ISO) models, SSAE 16 reports on controls at a service organization relevant to the user entities’ internal controls over financial reporting.

However, there was a growing need for third-party comfort over operational and compliance controls. The profession addressed this gap by developing Trust Services Principles, Criteria, and Illustrations
Trust Services provides criteria for evaluating and reporting on a system’s security, availability, processing integrity, protection of information designated as confidential, and maintenance of the privacy of personal information.

New Approach
The AICPA has embarked on a new approach to offer alternative solutions for reports designed to provide users of third-party services comfort around those business controls relevant to them: AICPA Service Organization Control (SOC) reports. There are three reports in this framework:

- **AICPA SOC 1**: Report on Controls at a Service Organization Relevant to User Entities’ Internal Control over Financial Reporting (provides comfort around financial reporting and transaction services)
- **AICPA SOC 2**: Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy
- **AICPA SOC 3**: Trust Services Report

Service organizations providing user entities comfort relevant to internal controls over financial reporting (ICFR) will take the SOC 1 report approach.

For users of cloud computing (as an example), the AICPA SOC 1 approach, testing financial reporting controls, provides little assurance regarding key controls around availability, reliability, confidentiality, and integrity of data. Such situations may best be served through the issuance of an AICPA SOC 2 report.

Service Organization Control Report 2
AICPA SOC 2 engagements will apply a risk-based approach for hosted-applications, software as a service (SaaS) and cloud computing spaces, where information security, availability, confidentiality, privacy and processing integrity of user data is more relevant.

AICPA SOC 2 reporting will give user entities transparency into service organizations by
providing independent assurance that processes and systems are:

- Adequately designed to achieve operational and compliance objectives
- Effective to achieve operational and compliance objectives

Note, guidance for SOC 2 reporting is not formally published at this time. To stay abreast of the latest developments, visit the Accounting & Auditing interest area of www.aicpa.org and select “Resources” then “Assurance Services.”

**Summary**

Today’s business environment is growing increasingly complex and, as a result, businesses look for strategic partners with the tools and technology available to deliver goods and services.

For the user entity that outsources a task or function to a service organization, it is important for the user entity to understand what they are buying.

An AICPA SOC 2 report enables a user entities’ management to carry out their internal control responsibilities related to the design and operating effectiveness of controls at the service organization, with regard to security, availability, processing integrity, confidentiality or privacy.

*SAS 70 was updated when the International Auditing and Assurance Standards Board (IAASB) developed International Standard for Attest Engagements (ISAE) 3402, providing international guidance for reporting on controls at service organizations. This international standard was developed concurrently with the Accounting Standards Board (ASB) convergence project, resulting in the promulgation of SSAE 16.*