AICPA®

Service Organization Controls

Managing Risks by Obtaining a Service Auditor's Report

Contributing Authors
Audrey Katcher, CPA, CITP, Partner at RubinBrown, LLP
Janis Parthun, CPA, CITP, Sr. Technical Manager — IMTA at AICPA
Curtis Stewart, CPA, CITP, Director at Deloitte & Touche, LLP

Technical Reviewers
Chris Halterman, CPA, Executive Director at Ernst & Young, LLP
Erin Mackler, CPA, Senior Technical Manager at AICPA
Tom Patterson, CPA, Associate Partner at IBM Global Business Svcs
Dan Schroeder, CPA, CITP, Partner at Habif, Arogeti, & Wynne, LLP
Steven Ursillo Jr., CPA, CITP, Director at Sparrow Johnson & Ursillo Inc.

This brochure was developed by the Service Organization Control Reporting Task Force of the AICPA's Information Management and Technology Assurance (IMTA) Executive Committee, in collaboration with the AICPA Assurance Services Executive Committee. The IMTA Executive Committee provides Section members with information, advocacy and leadership to help members enhance their understanding, use and management of technology from a CPA's unique perspective within the communities they serve. Visit **aicpa.org/IMTA** to learn more about IMTA Section membership.

The task forces involved in the development of the two Service Organization Control guides are:
- Service Organization Guide Task Force of the Auditing Standards Board
- Trust/Data Integrity Task Force of the Assurance Services Executive Committee
- Privacy Task Force of the Assurance Services Executive Committee/Information Management and Technology Assurance Executive Committee

Updated February 2013

Table of Contents

Reporting on a Service Organization's Controls: A Brief History

The American Institute of CPAs® (AICPA®) has long recognized the need for CPAs to understand the risks related to an entity's use of service organizations. Historically, guidance for CPAs reporting on controls at a service organization relevant to customers' internal control over financial reporting was primarily contained in Statement on Auditing Standards (SAS) No. 70, Service Organizations (AU Section 324 of the SASs).

Building Trust and Confidence in Third-Party Relationships

Today, it is common for entities to outsource to a service organization certain tasks or functions related to their business, even those that are core to their operations. When users of a service organization's services (user entities) outsource these tasks and functions, many of the risks of the service organization become risks of the user entities. In light of several prominent internal-control breakdowns (e.g., security and privacy breaches, and frauds) and increasing regulatory focus on internal control (e.g., Sarbanes-Oxley Act, Basel II, HITECH and HIPAA), user-entity management is increasing its due diligence for prospective service organizations and governance oversight of current service organizations. Technological, regulatory and other changes have heightened the need for information and assurance that enable management to demonstrate it has addressed stakeholder concerns related to the security, availability and processing integrity of the systems a service organization uses to process user entities' data, and the confidentiality and privacy of the information these systems process.

By engaging an independent CPA to examine and report on a service organization's controls, service organizations can respond to meet the needs of their user entities and obtain an objective evaluation of the effectiveness of controls that address operations and compliance, as well as financial reporting at those user entities. To provide the framework for CPAs to examine controls and to help management understand the related risks, the AICPA has established three **Service Organization Control (SOC)** reporting options (SOC 1, SOC 2 and SOC 3 reports).

When users of a service organization's services (user entities) outsource these tasks and functions, many of the risks of the service organization become risks of the user entities.

SOC 1 engagements are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization. SOC 1 reports focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. SOC 2 and SOC 3 engagements address controls at the service organization that relate to operations and compliance. SOC 1, 2 and 3 reports represent significant changes in service organization reporting approaches brought about as a result of several important changes. Among the changes:

- **Trust Services Principles, Criteria and Illustrations**, as updated, was effective for SOC 3 reports issued on or after Sept. 15, 2009.

- In December 2009, the International Auditing and Assurance Standards Board (IAASB) issued new International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization.

- Shortly thereafter, the AICPA issued SSAE No. 16, Reporting on Controls at a Service Organization (AICPA, Professional Standards, Vol. 1, AT sec. 801) (or SOC 1 report).

  – The replacement of SAS 70 with SSAE 16 represents the first significant modification to the AICPA standards for reporting on controls at a service organization since SAS 70 was issued in 1992.

  – As organizations became increasingly concerned about risks beyond financial reporting, SAS 70 often was misused as a means to obtain assurance regarding compliance and operations. SSAE 16 and ISAE 3402 were drafted to correct these misuses.

- The AICPA established a new guide for engagement performed in accordance with AT Section 101, Attest Engagements, of the attestation standards using the Trust Services Criteria (SOC 2 reports), to assist CPAs in reporting on the effectiveness of a service organization's controls related to operations and compliance. This new guide combines the Trust Services criteria (related to security, availability, processing integrity, confidentially or privacy) with the reporting detail provided by SSAE 16 to help service organizations provide their user entities with the information they desire.

By offering these three SOC reporting options, the AICPA seeks to address the needs of the marketplace and enable CPAs to protect the public.

As organizations became increasingly concerned about risks beyond financial reporting, SAS 70 often was misused as a means to obtain assurance regarding compliance and operations.

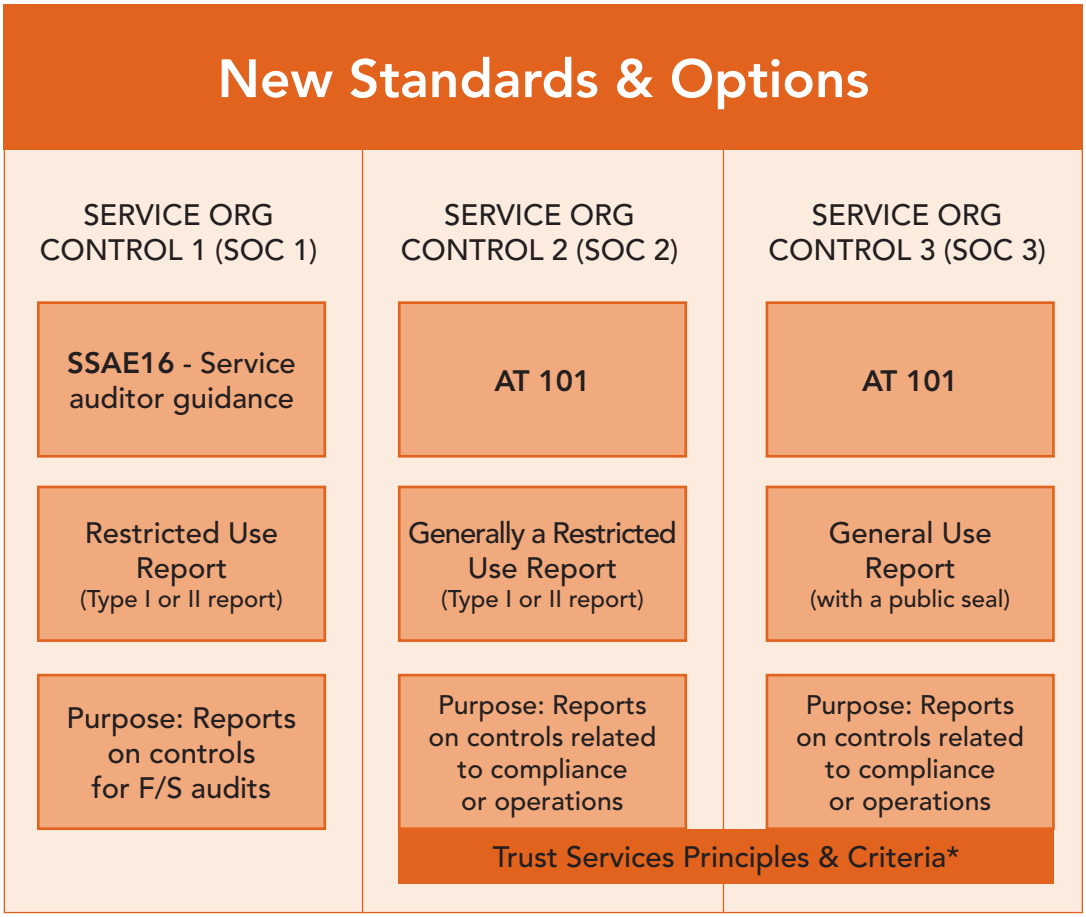
Historically

SAS 70 STANDARD	TRUST SERVICES PRINCIPLES & CRITERIA*
Service auditor guidance	SysTrust Report (with a public seal)
User auditor guidance	WebTrust Report (with a public seal)
Purpose: Reports on controls for F/S audits	Purpose: Reports on controls related to compliance or operations

Misconception: SAS 70 reports often were misinterpreted as a means to obtain assurance regarding controls over compliance and operations.

***Trust Services Principles & Criteria includes:**

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy



Definitions:

- A service auditor is a CPA who examines and reports on controls at a service organization.
- A user auditor is a CPA who performs an audit of the financial statements of an entity that uses a service organization and may need information about controls at the service organization.

AICPA Service Organization Control (SOC) Reports

SOC 1 Report: What is it?

Reports on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting: SOC 1 engagements are performed under SSAE 16, ***Reporting on Controls at a Service Organization***. SOC 1 reports are examination engagements undertaken by a service auditor to report on controls at an organization that provides services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting.

There are two types of SOC 1 reports:

- **Type 1** — A report on management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

- **Type 2** — A report on management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

Use of a SOC 1 report is restricted to existing user entities (not potential customers). Updated guidance for SOC 1 reports (SSAE 16) is effective for service auditors' reports for periods ending on or after June 15, 2011.

Putting a SOC 1 Report to Work

An employee benefit plan uses a bank trust department to invest and service the plan's assets. When the employee benefit plan's financial statements are audited, the plan's auditor needs information about the plan's internal control over financial reporting, including controls at the bank trust department that affect the employee benefit plan's financial statements. To help the auditor obtain that information, a CPA (service auditor) performs an examination of controls at the bank trust department resulting in a report with detailed information about those controls. The service auditor's report includes opinions on whether the description of the bank trust department's system is fairly presented and whether controls at the bank trust department that may affect user entities' financial reporting are suitably designed. A type 2 report also includes the service auditor's opinion on whether the controls were operating effectively and describes tests of the controls performed by the service auditor to form that opinion and the results of those tests. The auditor of the benefit plan's financial statements uses the service auditor's report to obtain information needed to audit the employee benefit plan's financial statements.

SOC 2 Report: What is it?

Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy: Many entities outsource tasks or entire functions to service organizations that operate, collect, process, transmit, store, organize, maintain and dispose of information for user entities. SOC 2 engagements use the predefined criteria in ***Trust Services Principles, Criteria and Illustrations***, as well as the requirements and guidance in AT Section 101, ***Attest Engagements*** (AICPA, ***Professional Standards***, Vol. 1). A SOC 2 report is similar to a SOC 1 report. Either a type 1 or type 2 report may be issued and the report provides a description of the service organization's system. For a type 2 report, it also includes a description of the tests performed by the service auditor and the results of those tests. SOC 2 reports specifically address one or more of the following five key system attributes:

- **Security** — The system is protected against unauthorized access (both physical and logical).
- **Availability** — The system is available for operation and use as committed or agreed.
- **Processing integrity** — System processing is complete, accurate, timely and authorized.
- **Confidentiality** — Information designated as confidential is protected as committed or agreed.
- **Privacy** — Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.

Putting a SOC 2 Report to Work

A Software-as-a-Service (SaaS) or Cloud Service Organization that offers virtualized computing environments or services for user entities and wishes to assure its customers that the service organization maintains the confidentiality of its customers' information in a secure manner and that the information will be available when it is needed. A SOC 2 report addressing security, availability and confidentiality provides user entities with a description of the service organization's system and the controls that help achieve those objectives. A type 2 report also helps user entities perform their evaluation of the effectiveness of controls that may be required by their governance process. Another example is a medical claims processing service organization that processes claims for health insurers (user entities) and wishes to assure those users that its controls over the processing of claims will protect the information in those claims, which is subject to privacy laws.

SOC 2 reports specifically address one or more of the following five key system attributes:

- *Security*
- *Availability*
- *Processing Integrity*
- *Confidentiality*
- *Privacy*

SOC 3 Report: What is it?

Trust Services Report for Service Organization: SOC 3 engagements use the predefined criteria in ***Trust Services Principles, Criteria and Illustrations*** that also are used in SOC 2 engagements.

The key difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report, which is generally a restricted-use report, contains a detailed description of the service auditor's tests of controls and results of those tests as well as the service auditor's opinion on the description of the service organization's system. A SOC 3 report is a general-use report that provides only the auditor's report on whether the system achieved the trust services criteria (no description of tests and results or opinion on the description of the system). It also permits the service organization to use the SOC 3 seal on its website. For more information about the SysTrust for Service Organization seal program go to webtrust.org.

For more details on difference between a SOC 2 report and a SOC 3 report, refer to *Guide:* ***Reporting on Controls at a Service Organization (SOC 2℠)***.

SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity, confidentiality and privacy).

Putting a SOC 3 Report to Work

Companies that use a business partner to perform part of their operations for selling goods via the Internet often find that their customers are concerned with the privacy of the information they provide to the company and the business partner. Since many customers would like assurance about how the privacy of that information is being managed and processed, the business partner service organization can use a SOC 3 report to address such concerns. For example, a large online retailer may establish an affiliates program that permits small specialist retailers to use the transaction processing systems of the online retailer. Because of the concern that many customers (of the specialist retailers) may have regarding the online retailers collection and use of purchase information, the online retailer and the specialist retailers wish to assure customers that the online retailer maintains the privacy of customers' information. Management of the online retailer may request a SOC 3 engagement, performed by a CPA over the system or processing using the Trust Services Principles and Criteria, and may then distribute the SOC 3 report to customers via a link on its website and publicly display the SOC 3 Report: SysTrust for Service Organizations seal.

A SOC 3 report is a general-use report that provides only the auditor's report on whether the system achieved the trust services criteria. It also permits the service organization to use the SOC 3 seal on its website.

SOC Summary Chart (With Suggested Guidance):			
	SOC 1 Report	**SOC 2 Report**	**SOC 3 Report**
Kind of controls addressed by the report	Controls likely to be relevant to user entities financial statements	Controls over the security, availability and processing integrity of a system and the confidentiality and privacy of information processed by the system	Controls over the security, availability and processing integrity of a system, and the confidentiality and privacy of information processed by the system
Standard under which the engagement is performed and other related guidance	SSAE No. 16, Reporting on Controls at a Service Organization AICPA Guide. Service Organizations, Applying SSAE No. 16 (SOC 1℠)	AT 101, Attestation Engagements AICPA Guide, Reporting on Controls at a Service Organization (SOC 2℠)	AT 101, Attestation Engagements AICPA Technical Practice Aid, Trust Services Principles, Criteria and Illustrations
Content of report	Description of service organization's system CPA's opinion on fairness of presentation of the description, suitability of design and in a type 2 report, the operating effectiveness of controls A type 2 report includes a description of the CPA's tests of controls and results	Description of service organization's system CPA's opinion on the fairness of presentation of the description, suitability of design and in a type 2 report, the operating effectiveness of controls A type 2 report includes a description of the CPA's tests of controls and results	An unaudited system description used to delineate the boundaries of the system CPA's opinion on whether the entity maintained effective controls over its system

Making The Right Choice

By helping to increase customer trust and helping customers to address their risk and governance concerns, these reports provide value to service organizations — but it's important to understand the unique aspects of what the SOC report offers and match those aspects to user needs. Making the right choice can help ensure that an organization will receive the most effective solution and the most value for its money.

User entities that would like to undergo a SOC 1, SOC 2 or SOC 3 engagement may find it helpful to look for CPA firms with this SOC logo displayed on their website.

Service organizations that had a SOC 1, SOC 2 or SOC 3 engagement within the past year may register with the AICPA for the use of this logo to be displayed.

In summary, to determine the most appropriate SOC report for your purposes, a service organization should:

1. Understand the needs of user entities:

   A. Are they focused on internal control over financial reporting? Then a SOC 1 report is most appropriate.

   B. Are key compliance and operational controls (such as those related to security, availability, processing integrity, confidentiality or privacy) of primary interest? Then a SOC 2 or SOC 3 report may be most appropriate.

2. Understand the best communication mechanism for your users:

   A. Are they in need of detail about your systems and processes? Then a SOC 1 or SOC 2 report may be most appropriate.

   B. Will the posting of a summary report/seal suffice? Then a SOC 3 report may be most appropriate.

To learn more about Service Organization Control reporting, go to:

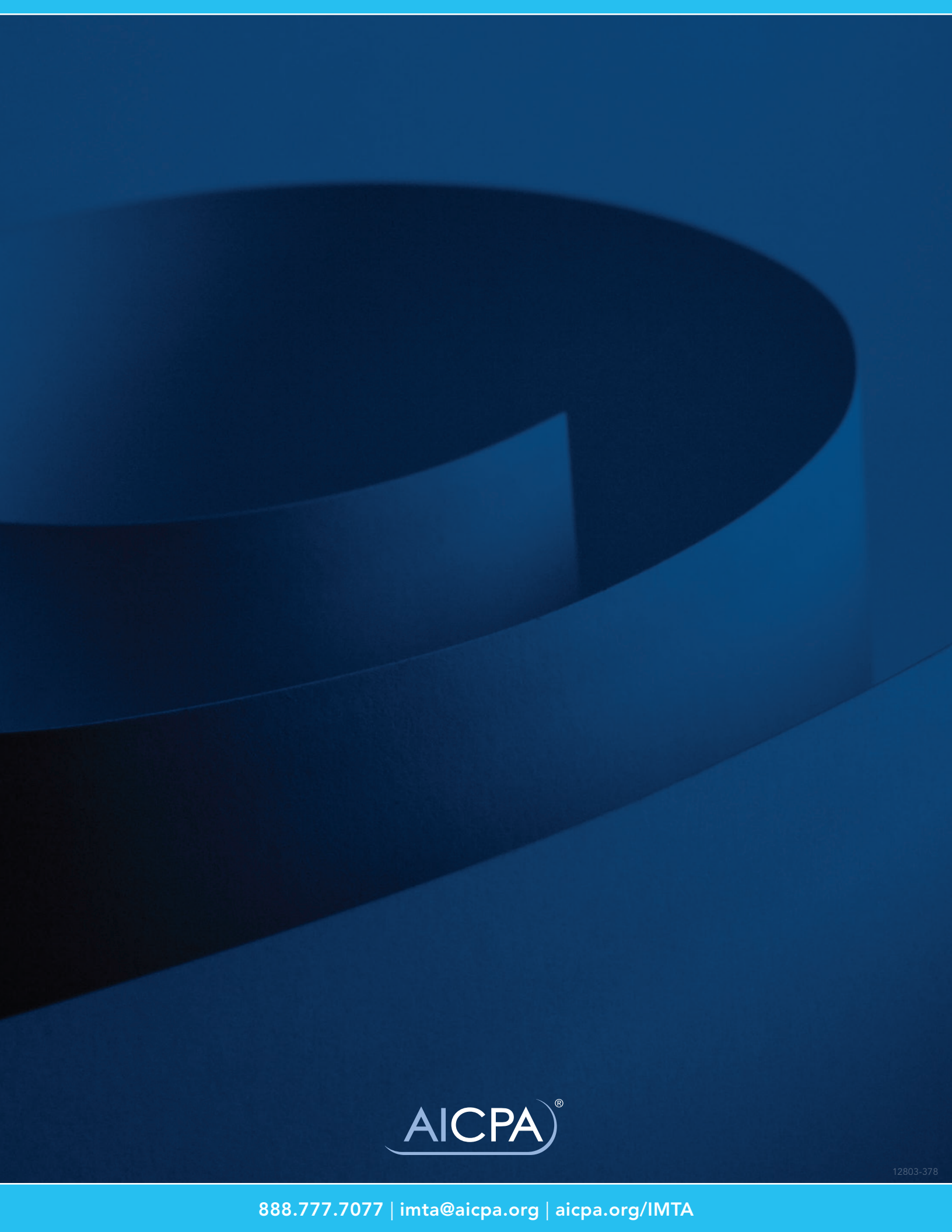
aicpa.org/SOC
AICPA's Information Management and Technology Assurance Interest Area (aicpa.org/IMTA)

To purchase AICPA products related to Service Organization Control reporting, please visit cpa2biz.com.

	AICPA Member	IMTA Section Member	CITP Credential Holder
Who it's for	CPAs or non-CPAs who do not provide information management and technology assurance services	CPAs who practice in the following areas: - Risk Assessment - Fraud Considerations - Internal Controls - IT Audit & Attestations - Information Management and Business Intelligence	CPAs specializing in information management and technology assurance with knowledge and expertise through education, experience and exam requirements
Discounts on CPE, Events and Publications			
Web seminars led by top Information Management and Technology Assurance experts		✓ (in addition to AICPA membership discount)	✓ (in addition to AICPA membership discount)
Complete Guide to the CITP Body of Knowledge		✓	✓
SOC 1 and SOC 2 Guide		✓	✓
IFRS COMPASS: IT Systems Implications		✓	✓
Vendor Product Discounts			
Information Active, Inc. (Active Data Products)		✓	✓
Audimation Services (IDEA Products)		✓	✓
Actuate (Birt OnDemand)		✓	✓
CITP Credential and Pathway			
CITP Marketing Toolkit			✓
CITP Pathway		✓	✓
Find a CITP database			✓
Media, speaking and writing opportunities			✓
Cost	**$205-$395** (Varies depending on firm status)	**$200** (look for discounts by attending conferences and other AICPA IMTA events!)	**$350**

* Note: This is a highlight of benefits available. All benefits are not included in this listing.

Notes



12803-378

888.777.7077 | imta@aicpa.org | aicpa.org/IMTA