System and Organization Controls (SOC)

AICPA

# CPAs: Helping service organizations build trust and transparency

**Disclaimer:** The contents of this publication do not necessarily reflect the position or opinion of the American Institute of CPAs, its divisions and its committees. This publication is designed to provide accurate and authoritative information on the subject covered. It is distributed with the understanding that the authors are not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

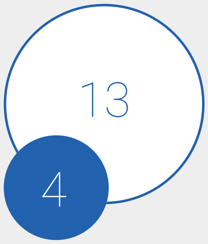
# Contents

# Build trust and transparency

**Cloud computing. Outsourced functions. Competition. Cybersecurity threats. Compliance requirements.**

Is your organization demonstrating its commitment to maintain effective internal controls and safeguards to protect not only yourself but your customers? Outsourced services users and their auditors increasingly are requesting more information than ever before about the effectiveness of controls at the service organizations they use, or are considering using, for outsourced business functions.

Using the AICPA's various SOC for Service Organizations offerings, CPAs can provide assurance reports that provide your users the valuable information they need to assess and address the risks associated with the outsourced services you provide, helping build trust and transparency.



4 of the leading 13 information security and cybersecurity consultants are CPA firms.

CPA firms deploy multidisciplinary teams composed of licensed CPAs and information technology and security specialists to ensure a comprehensive and thorough evaluation of controls related to the services you provide.

(Source: Whitworth, Martin. "The 13 Global Providers That Matter Most and How They Stack Up." The Forrester Wave™: Information Security Consulting Services, Q1 2016. Jan. 29, 2016

# What are SOC for Service Organizations reports?

**SOC for Service Organizations reports are internal control reports, which independent CPAs provide, on the services a service organization provides.**

- Useful for evaluating the effectiveness of controls related to the services performed by a service organization
- Appropriate for understanding how the service organization maintains oversight over third parties that provide services to customers
- Help reduce compliance burden by providing one report that addresses the shared needs of multiple users
- Enhances the ability to obtain and retain customers

Service providers don’t conduct a SOC examination just because they want one. They request a report because user entities and their respective auditors demand them.

(Source: Moss Adams LLP. *Why a SOC Report Makes All the Difference.* Igniting Growth: SOC Reporting.)

# Types of SOC for Service Organizations Reports

The variety of SOC for Service Organizations offerings available include:

- *SOC 1® — SOC for Service Organizations: ICFR —* These reports are specifically designed to address controls at the service organization that are relevant to the user entities' financial statements. They enable user auditors to perform risk assessment procedures and obtain audit evidence about whether controls at the service organization are operating effectively. Use of these reports is restricted to management of the service organization, user entities, and user auditors.
- *SOC 2® — SOC for Service Organizations: Trust Services Criteria —* These reports address controls relevant to security, availability and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information these systems process. They provide a level of detail sufficient to address the user's vendor risk management needs and are restricted to specified parties with sufficient knowledge and understanding of the service organization's system and the nature of services it provides. Use of these reports generally is restricted to service organization management, user entities of the system, business partners, CPAs providing services to user entities and business partners, and regulators.
- SOC 3® — SOC for Service Organizations: Trust Services Criteria for General Use Report — Like SOC 2, these reports address controls relevant to security, availability, processing integrity, confidential and privacy. However, they do not provide the same level of detail. Therefore, they are considered general use reports and can be freely distributed.

For more information about SOC 1, SOC 2, and SOC 3 reports, visit aicpa.org/soc4so.

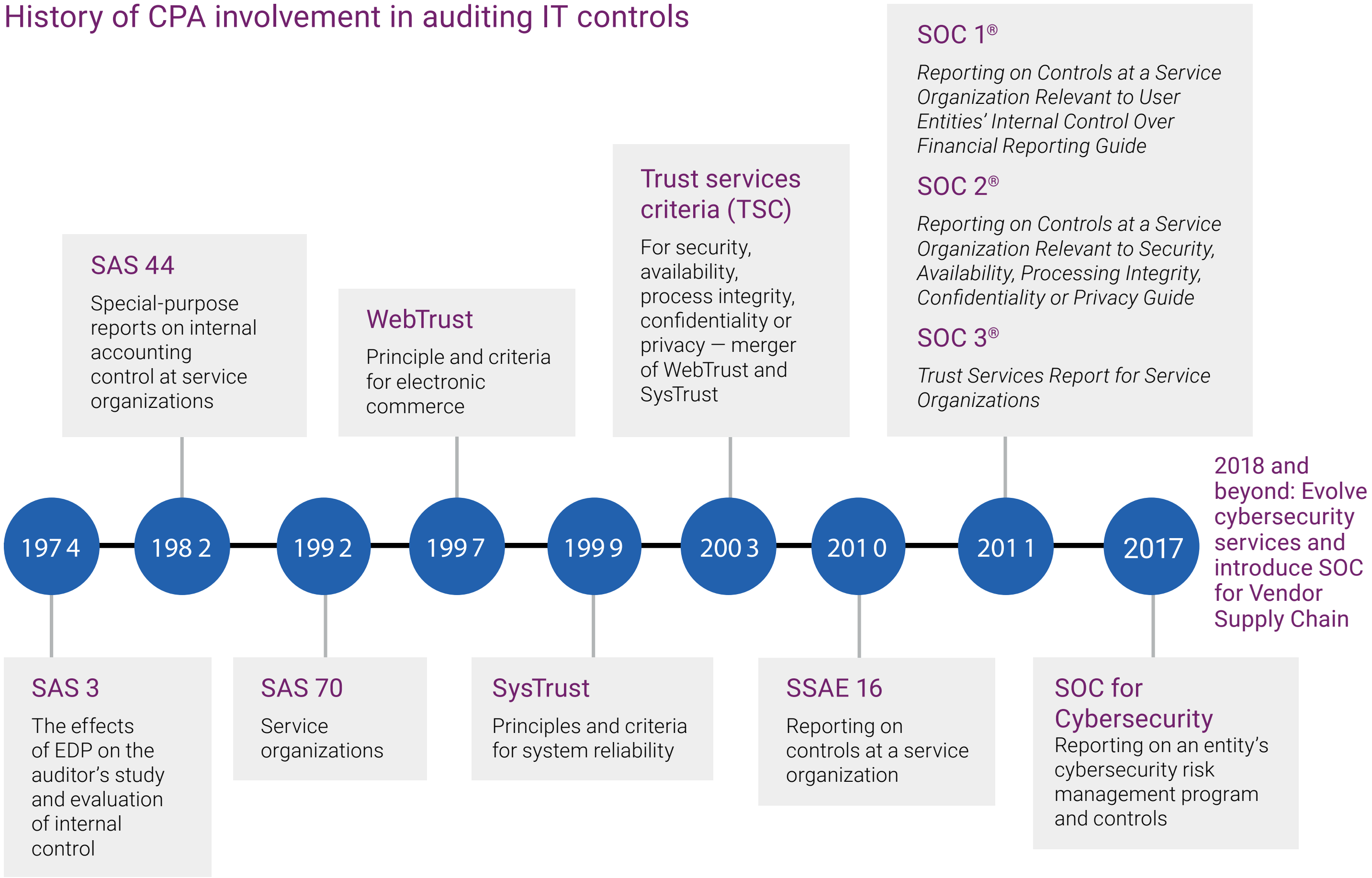
# Why CPA firms? Education, experience and expertise

The education, experience and expertise of CPAs position them as the premier providers of SOC for Service Organizations services.

- Knowledge of relevant IT systems and technology, including mainframes, networking, firewalls, network management systems, security protocols and operating systems
- Understanding of IT processes and controls, such as management of operating systems, networking and virtualization software and related security techniques; security principles and concepts; software development; and incident management and information risk management
- Experience with common security and cybersecurity publications and frameworks
- Expertise in evaluating processes, control effectiveness and providing advisory and assurance services relating to these matters
- Multidisciplinary teams that incorporate certified information security professionals such as Certified Information Systems Security Professionals (CISSP), Certified Information Systems Auditors (CISA) and Certified Information Technology Professionals (CITP®)
- Proficiency in measuring performance against established criteria, applying appropriate procedures for evaluating against those criteria and reporting results
- Strict adherence to service-specific professional standards, professional code of conduct and quality control requirements
- Holistic understanding of entity's industry and business, including whether the industry in which the entity operates is subject to specific types of or unusual cybersecurity risks and uses specific industry technology systems
- Objectivity, credibility and integrity
- Independence, professional skepticism and commitment to quality
- Strong analytical skills
- International perspective for global organizations

# CPAs: Forerunners in the cybersecurity movement

## History of CPA involvement in auditing IT controls



1974

**SAS 3**
The effects of EDP on the auditor's study and evaluation of internal control

1982

**SAS 44**
Special-purpose reports on internal accounting control at service organizations

1992

**SAS 70**
Service organizations

1997

**WebTrust**
Principle and criteria for electronic commerce

1999

**SysTrust**
Principles and criteria for system reliability

2003

**Trust services criteria (TSC)**
For security, availability, process integrity, confidentiality or privacy — merger of WebTrust and SysTrust

2010

**SSAE 16**
Reporting on controls at a service organization

2011

**SOC 1®**
*Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting Guide*

**SOC 2®**
*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy Guide*

**SOC 3®**
*Trust Services Report for Service Organizations*

2017

**SOC for Cybersecurity**
Reporting on an entity's cybersecurity risk management program and controls

2018 and beyond: Evolve cybersecurity services and introduce SOC for Vendor Supply Chain

**1970s** – CPAs required to consider effects of electronic data processing on the evaluation of internal control in financial statement audits.

**1990s** – CPAs begin performing SAS 70 audits to report on the effectiveness of internal control over financial reporting.

**2000s** – CPAs begin using the trust services criteria for evaluating controls relevant to security, availability, processing integrity, confidentiality and privacy and issuing SOC reports to address vendor management needs related to outsourced services.

**2017** – Introduction of SOC for Cybersecurity attestation services for CPAs to report on the effectiveness of controls within an organization's cybersecurity risk management program.

**2018 and beyond** – Continue to evolve cybersecurity services and introduce SOC for Vendor Supply Chain to enable users of products produced, manufactured and distributed by an entity to better understand and manage risks, including cybersecurity risks, arising from their business relationships with the entity.

AICPA®

P: 919.402.4500 | F: 919.402.4505 | W: aicpa.org