SOC for Cybersecurity

Helping you 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.

For more information about the procedure for requesting permission to make copies of any part of this work, please email copyright@aicpa.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, 220 Leigh Farm Road, Durham, NC 27707–8110.
CPAs and cybersecurity: Helping you build trust and transparency


Is your organization prepared for a cybersecurity attack? Boards of directors, senior management and other stakeholders are requesting more information than ever before about organizations’ cybersecurity risk management programs.

Using the AICPA’s SOC for Cybersecurity framework, CPAs can provide assurance over the effectiveness of controls within your organization’s cybersecurity risk management program, helping build trust and transparency for customers, investors and leadership.

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 your cybersecurity risk management program and its effectiveness in meeting your organization’s cybersecurity objectives.
What is SOC for Cybersecurity?

The SOC for Cybersecurity examination provides an independent, entity-wide assessment of your organization’s cybersecurity risk management program.

- Appropriate for businesses, not-for-profits and virtually any other type of organization
- Helps reduce uncertainty and build resilient organizations by evaluating effectiveness of existing cybersecurity processes and controls
- Permits flexibility by not constraining management to a particular security management framework or control framework
- Results in a general use report on whether:
  - The description of an entity’s cybersecurity risk management program is presented in accordance with description criteria and
  - The controls within that program were effective in achieving the entity’s cybersecurity objectives

62% of executives expect to see an increase in reporting requests from their board of directors on cybersecurity program effectiveness.

(Source: Deloitte, 2018. “Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year.”)
AICPA cybersecurity risk management reporting framework

The AICPA cybersecurity risk management reporting framework helps organizations communicate about the effectiveness of their cybersecurity risk management programs via three components:

• **Description Criteria for Management’s Description of an Entity’s Cybersecurity Risk Management Reporting Program** — This is used by management to provide transparency regarding its cybersecurity risk management program and used by CPAs to report on management’s description. Management’s description provides users of the report with information that can help them understand the entity’s cybersecurity risks and how it manages those risks. Description criteria includes considerations on the nature of an entity’s business and operations, factors affecting inherent cybersecurity risk, risk governance and assessment process and the monitoring of the cybersecurity program, among other criteria.

• **2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy** — This is used by management to evaluate the effectiveness of controls and used by CPAs providing advisory or attestation services to evaluate and report on the effectiveness of controls within the cybersecurity risk management program.

• **AICPA Guide Reporting on an Entity’s Cybersecurity Risk Management Program and Controls** — This attestation guidance assists CPAs engaged to examine and report on an entity’s cybersecurity risk management program (SOC for Cybersecurity). This guide also contains information that can assist management in understanding the SOC for Cybersecurity engagement and its responsibilities with respect to the engagement.
Why CPA firms?
Education. Experience. Expertise.

The education, experience and expertise of CPAs position them as the premier providers of SOC for Cybersecurity 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 cybersecurity publications and frameworks (NIST CSF, ISO 27001/27002, 2013 COSO Internal Control — Integrated Framework, COBIT 5, etc.)

• Expertise in evaluating processes, control effectiveness and providing advisory 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

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 or 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.
