

System and Organization Controls (SOC)

SOC refers to **System and Organization Controls** and ACT conducts SOC examinations following the American Institute of Certified Public Accountants (AICPA) standards referenced as AT-C. Four separate engagements we perform include:

SOC for Cybersecurity is applicable to all entities and involves an examination of an entity's cybersecurity risk management program and related controls.

SOC 1 is for service organizations and is an examination of controls related to financial reporting. Report distribution is restricted.

SOC 2 is for service organizations and is an examination of controls relevant to security, availability, processing integrity, confidentiality, and privacy. Report distribution is restricted.

SOC 3 is for service organizations and results in an abbreviated report for general use.

A Comparison

A high level comparison of the SOC suite of attestation engagements follows:

SOC for Cybersecurity	SOC 1	SOC 2	SOC 3
For all entities	For service organizations	For service organizations	For service organizations
Entity level controls	Financial reporting controls	System level controls	System level controls
Reports broader level risks	Reports detailed control info	Reports detailed control info	Report less detailed
Can be general use	Restricted use	Restricted use	General use
Audience is entity stakeholders	Audience is user entities / auditors	Audience is user entities / auditors	Audience is interested parties
Includes disclosures about key controls, but not a testing matrix	Includes a controls testing matrix	Includes a controls testing matrix	Includes a brief description, assertion & auditor opinion

ACT Cybersecurity Services

Readiness Assessment. Our professionals perform a readiness assessment evaluating your description, controls, and/or your risk management program in comparison to a defined framework, such as the applicable trust services criteria or the National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF), with the goal of providing management with observations and recommendations to enhance your description, controls, and/or your cybersecurity risk management program and prepare for an attestation examination and report.



**Arnett
Carbis
Toothman** LLP
CPAs & Advisors

actcpas.com

System and Organization Controls (SOC) continued...

Continued...

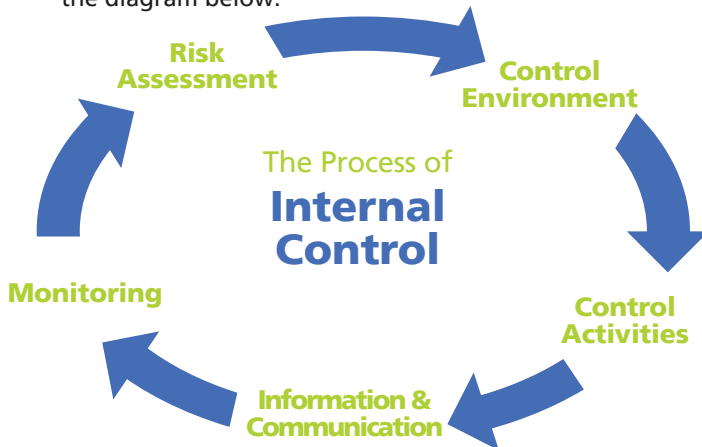
Examination and Reporting. Our professionals complete the SOC for Cybersecurity, SOC 1, SOC 2, or SOC 3 examination and attestation reporting using the criteria from a defined framework, which can be provided to key stakeholders.

Why Are Controls Important?

Properly operating systems should make it easier to sleep at night - good controls are what sustain businesses and just might keep a business death event from happening.

What are the Primary Elements of Internal Control?

There are five fundamental components of **Internal Control**. Their relationship to one another is depicted in the diagram below:



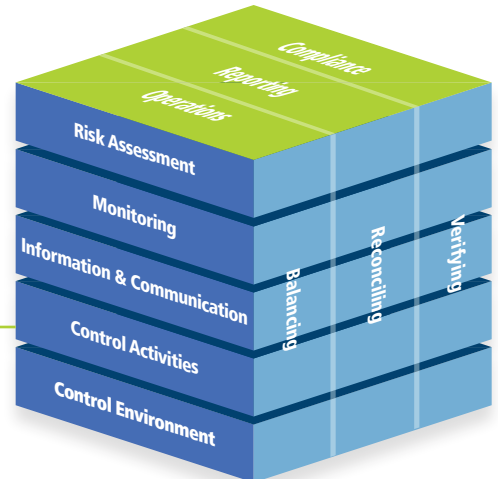
Lane Ellis, Jr., CPA, CISA, CVA, ABV, CGMA; Partner
Email: lane.ellis@actcpas.com

Christopher E. Joseph, CPA, CISA, CRISC, CITP; Partner
Email: chris.joseph@actcpas.com

Lisa S. Stover, CPA, CITP, CISA, CGMA; Senior Manager
Email: lisa.stover@actcpas.com

Phone: 800.642.3601 or 304.346.0441

The Elements of Control Structure



Those charged with governance appreciate the critical interaction of the system elements illustrated by the Systems Element Structure.

The five elements depicted along the diagram's left side are foundational components in control systems. Activities such as balancing, reconciling, and verifying are examples of system checkpoints.

As entities continually strive toward achieving business goals, these elements are in constant interaction with operating, reporting, and compliance functions.

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. The AICPA SOC 3 report is designed for prospective use and it is the only one that can be disclosed widely, even on a company website.

Arnett Carbis Toothman's understanding of these system elements remains foundational to our success in providing examinations for all types of service organizations. The ACT team uses its broad understanding of the business process and its command of technology and security applications to deliver examination reports that are accurate and thorough.

Arnett Carbis Toothman's consulting services teams possess a wealth of experience in multiple industries. Our teams are results-driven and seek long-term solutions to the challenges facing businesses today.

ACT *with confidence*