SOC FOR CYBERSECURITY.

SOC for Cybersecurity is the AICPA's entity-wide attestation, introduced in April 2017. Management describes its whole cybersecurity risk management program against the description criteria, asserts that controls met its objectives, and a CPA opines on both. **One opinion on the whole program, built to be shared.**

ENTITY-WIDE, NOT A SYSTEM | GENERAL USE REPORT | 19 CRITERIA, 9 CATEGORIES | INTRODUCED APRIL 2017

01 THE MECHANISM

The Whole Program in Scope

The examination is generally performed on an entity-wide cybersecurity risk management program, though scope may narrow to a unit or function. Management answers for every control, whether the entity or a third party performs it, **so there is no carve-out**. [02] [06]

Two Criteria, One Report

Management writes the description against the description criteria (DC section 100) and judges its controls against control criteria: the trust services criteria for security, availability and confidentiality, or other suitable criteria. **The CPA opines on both.** [07] [03] [08]

Written for General Use

The purpose is to give general users useful information about the program and its controls: management, directors, analysts, investors and others. The report is **appropriate for general use**, though a practitioner may restrict it, and it prints no tests. [02] [06]

02 THE FLOW

How the Report Is Built DESCRIBE

1. **Set the objectives and the boundary:** management establishes the entity's cybersecurity objectives for availability, confidentiality, integrity of data and integrity of processing, identifies the risks to them and designs controls. The opinion is measured against them. [02] [03]
2. **Describe the program against DC 100:** nineteen criteria in nine categories, from the business and the information at risk to governance, risk assessment, monitoring and control processes. Significant incidents of the prior twelve months are disclosed. [02] [03]
3. **Assert, then be examined:** management names the description and control criteria in a written assertion, evaluates its controls and asserts both presentation and effectiveness. The CPA examines under AT-C sections 105 and 205 and opines on the period. [02] [03] [09]

How to Read One READ

1. **Find the three sections:** management's assertion, the independent accountant's report and the description. The opinion says two things: the description follows the description criteria, and the controls were effective to achieve the objectives over the period. [03] [02]
2. **Check which criteria and whose objectives:** the accountant's report names the control criteria used. Effectiveness is relative to objectives management set for itself, so read them before the opinion. A program built on NIST CSF or ISO/IEC can still be judged on the TSC. [03] [08]
3. **Weigh the limits the report states:** both the assertion and the opinion say the program gives reasonable, but not absolute, assurance; vendor failures, product vulnerabilities and persistent attackers are named. Projections to later periods are at risk; note the period end. [03]

03 DESCRIPTION CRITERIA CATEGORIES

CATEGORY	WHAT THE DESCRIPTION COVERS
Business	Nature of business and operations, and nature of information at risk (DC1–DC2): products, channels, data.
Objectives	Program objectives (DC3–DC4): the principal cybersecurity objectives and how they are set and approved.
Risk factors	Factors affecting inherent risk (DC5–DC6): technologies, providers, channels, change, incidents.
Governance	Governance structure (DC7–DC10): ethics, board oversight, accountability and reporting lines, staff.
Assessment	Risk assessment, communications and information quality (DC11–DC14): risks, vendors, reporting.
Controls	Monitoring and control processes (DC15–DC19): evaluations, escalation, responses, architecture, policies.

04 WAYS TO SHOW A CYBER PROGRAM

APPROACH	CPA OPINION ON THE PROGRAM?	WHAT IT MEANS
Questionnaire	No	Management's own answers to a buyer's checklist; no stated criteria, no independent examination, a new form for each customer.
Penetration test	No	Technical testing of chosen systems at a point in time; it finds exploitable weaknesses, not whether the program is governed.
SOC 2 Type 2	No	CPA opinion on one service system against the trust services criteria, with tests and results; restricted to parties who know it.
SOC for Cyber	Yes	CPA opinion that the description meets DC 100 and controls met the entity's objectives over the period; appropriate for general use.

SOC FOR CYBERSECURITY.

DESCRIBE · ASSERT · OPINE

05 PROGRAM OPERATIONS

Write objectives you can be measured against. The opinion says controls were effective to achieve the entity's cybersecurity objectives, so vague objectives weaken it. Derive them from business objectives, cover availability, confidentiality and integrity, and approve them. [03] [02]

Own every third-party control. There is no carve-out: the description must address all controls in the program, including those a vendor or partner performs. Keep the vendor risk process the criteria call for, tier suppliers by access and data, and collect their reports. [02] [03]

Keep an incident ledger built for disclosure. DC6 requires disclosure of incidents identified in the twelve months before period end that significantly impaired the objectives, with nature, timing, extent and disposition. Settle the threshold with counsel before fieldwork. [03] [02]

Pick the criteria and the audience first. General use means investors, analysts and regulators may read it, so decide whether the trust services criteria or another suitable framework fits, and whether to restrict use. The AICPA guide also covers readiness and design-only work. [04] [06]

06 CONTROL MAPPING

`TSC AS CONTROL CRITERIA`

The AICPA names the security, availability and confidentiality criteria of TSP section 100 (2017, points of focus revised 2022) as suitable control criteria, and the illustrative report uses them. The criteria are covered in the SOC 2 brief; here they test controls against the objectives. [08] [03] [02]

`NIST CSF, ISO 27001`

The framework is flexible: management may use criteria other than the trust services criteria as control criteria, such as the NIST Cybersecurity Framework or ISO 27001/27002, if appropriate for the engagement under the attestation standards. Other suitable description criteria are allowed. [06] [02]

`SSAE 18 & THE 2024 GUIDE`

The examination runs under AT-C sections 105 and 205 of the attestation standards, codified from SSAE No. 18 as amended; the AICPA's August 2026 compilation is current. The 2024 edition of the AICPA guide incorporates SSAE No. 20 on materiality and SSAE No. 21 on direct examinations. [02] [09] [04]

`SOC 2 (SYSTEM-LEVEL)`

The AICPA's own comparison: a SOC 2 examines a system that provides services, uses the trust services criteria, prints tests and results, and is restricted to parties who know it. SOC for Cybersecurity examines the entity-wide program, allows other criteria, omits test detail, and is general use. [05] [06]

07 WHAT THIS DOES NOT SOLVE

Not a Breach Shield
By its own terms the program offers **reasonable, but not absolute, assurance** against security events. [03]

Not a System Report
It covers the entity's program, not one service system; **a SOC 2 reports on a system**. [05] [06]

Not a Test Log
The practitioner's report carries an opinion; **tests of controls and their results are not included**. [02]

Not a Mandate
A voluntary, market-based framework; **no law or regulator requires the examination**. [06] [05]

08 MYTHS VS. REALITY

MYTH	REALITY
"It is just a SOC 2 for the whole company."	Different criteria and audience: **DC 100, entity-wide scope, general use**; SOC 2 covers a system. [05] [02]
"It must use the trust services criteria."	They are suitable control criteria, but **other suitable criteria, such as NIST CSF**, may serve instead. [06] [02]
"A clean opinion means nothing bad happened."	Assurance is reasonable, not absolute, and **significant incidents of the prior year are disclosed**. [03]
"Only service organizations can get one."	Any type of organization may be examined; **the responsible party is entity management**. [02] [01]
"The report cannot leave the company."	It is appropriate for general use; **practitioners may choose to restrict it**, but the design is open. [02]

09 SPEAK THE PROGRAM — KEY TERMS

`DESCRIPTION CRITERIA`
DC section 100: **19 criteria in nine categories** for management's description.

`CONTROL CRITERIA`
What controls are judged against: **the TSC or other suitable criteria** management picks.

`CYBERSECURITY OBJECTIVE`
An objective management sets for the program; **the opinion measures controls against it**.

`MANAGEMENT'S ASSERTION`
Written statement that the description follows DC 100 and **the controls were effective**.

`GENERAL USE`
A report whose use is **not restricted to specified parties**; a CPA may still restrict it.

`READINESS ENGAGEMENT`
A non-attestation engagement to prepare for the examination; **no opinion is issued**.