AICPA

# What are you doing to prevent cyberattacks?

## SOC 2® and SOC for Cybersecurity: How they're different and how they can help.

Cybersecurity is a top priority for many organizations. This is no surprise, considering the high number of attacks they face. An Accenture survey found that the average organization was a victim to 2.5 successful cyberattacks each week in FY 2017.*

In response, organizations are increasing their cybersecurity budgets, hiring more IT staff, deploying third-party solutions and providing more training for existing employees.

The SOC for Cybersecurity examination provides an independent, entity-wide assessment of these and other efforts — giving boards, investors, business partners and other stakeholders confidence in an organization's cybersecurity risk management program (CRMP).

The SOC 2 engagement can also provide users with insight into an organization's cybersecurity controls, but there are significant differences between the audience, subject matter and scope of each service.

* Accenture. 2017 Cost of Cyber Crime Study.

# What type of organization is being examined?

| If the organization is a … | Consider a … |
|---|---|
| Service organization | SOC 2 |
| Business, not-for-profit and virtually any other type of organization | SOC for Cybersecurity |

# Report

| | | SOC for Cybersecurity | SOC 2 |
|---|---|---|---|
| Users | | Entity management, directors, investors, business partners and other stakeholders | Service organization management and specified parties, such as user entities of the system and business partners that interact with the system |
| Purpose | | Provide general users with information about entity's CRMP. | Provide specific users with information about controls related to security, availability, processing integrity, confidentiality or privacy. |
| Level | | Entity-wide | System |
| Control criteria | | AICPA Trust Services Criteria (or other suitable criteria such as NIST CSF or ISO 27001) | AICPA Trust Services Criteria |
| Tests of controls and results of tests | | Performed, but details not included in the report | Performed, and details included in type 2 report |
| Contents | Description of | Entity's CRMP | Service organization's system |
| | Management's assertion | Whether: (a) the description of the CRMP was presented in accordance with the description criteria, and (b) controls within the CRMP were effective in achieving the entity's cybersecurity objectives | Whether: (a) the description of service organization's system was presented in accordance with the description criteria, and (b) the controls stated in the description were suitably designed and operating effectively to provide reasonable assurance that the organization's service commitments and system requirements were achieved based on the applicable trust services criteria |
| | CPA's report | Whether: (a) the description of the entity's CRMP was presented in accordance with description criteria, and (b) the controls within that CRMP were effective in achieving the entity's cybersecurity objectives | Whether (a) the description of the organization's system was presented in accordance with the description criteria, and (b) the controls stated in the description were suitably designed and operating effectively to provide reasonable assurance that the organization's service commitments and system requirements were achieved based on the applicable trust services criteria |

For more information, check out *SOC 2® examinations and SOC for Cybersecurity examinations: Understanding the key distinctions* at aicpa.org/SOC.

AICPA®

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