

# SOC compliance and attestations

A System and Organization Controls report (SOC 1, 2, or 3 report), governed by the AICPA, is a widely recognized attestation that allows organizations to demonstrate control maturity against their security posture. SOC are customizable to ensure applicability to the commitments each organization is responsible for and drives trust and confidence for their end users.

Coalfire Controls is a fully licensed, accredited CPA firm and affiliate of Coalfire that helps organizations examine and report on controls, allowing them to better respond to and meet the expectations of user entities. Our team offers the following related services:

## Readiness assessments

During a readiness assessment, we help identify and document your controls, determine any gaps that need to be remediated prior to pursuing a Type 1 or Type 2 report, and provide recommendations on how to remediate the gaps identified.

## Type 1 reports

We conduct a formalized SOC examination and report on the suitability of design and implementation of controls at a specific point in time.

## Type 2 reports

We conduct a formalized SOC examination and report on the suitability of design and operating effectiveness of controls over a period of time (typically at least six months). A Type 2 report requires sample testing several controls – such as HR functions, logical access, and change management – to ensure the

controls in place were operating effectively during the examination period.

## Other frameworks

Leveraging our expertise across a wide variety of frameworks, we can couple your SOC 2 report with other efforts to reduce audit fatigue and even provide a combined report (e.g., SOC and HIPAA or SOC and CSA STAR).

## Types of attestations

In addition to SOC attestations, including SOC 1, SOC 2, SOC 3, SOC for Cybersecurity, and SOC for Supply Chain, we provide support for the following attestations:

### Cloud Security Alliance's Security Trust & Assurance Registry (CSA STAR) attestation

Utilizes the SOC 2 framework to report on the suitability of the design and operating effectiveness of a cloud service provider's (CSP's) controls relevant to the applicable Trust Security Criteria (TSC) – including Security, Availability, Confidentiality, Processing

Integrity, and Privacy – and the suitability of the design and operating effectiveness of its controls in meeting the criteria in the CSA Cloud Controls Matrix (CCM).

### C5 attestation

Addresses the cloud computing compliance criteria catalogue (C5) developed by the Federal Office for Information Security in Germany (Das Bundesamt für Sicherheit in der Informationstechnik or BSI).

### Agreed-upon procedures

For other subject matter, we can issue reports based on agreed-upon procedures under SSAE standards. In conducting these engagements, our objectives would be to:

- Apply procedures that are established by the specified parties.
- Issue a written practitioner's report that describes the procedures and findings.

### Why Coalfire

- **We have more than 20 years of cybersecurity and service compliance expertise**, assessing more than 2,000 organizations and completing more than 400 SOC assessments annually.
- **Our dedicated team of SOC specialists** ensures we provide the best guidance to handle the most complex scenarios.
- **We work with the industry's largest cloud service providers** (e.g., Amazon, IBM, Microsoft), and 75% of our SOC engagements are facilitated for CSPs (e.g., SaaS, IaaS, PaaS). We leverage the knowledge from these engagements to help clients that are in the cloud or are interested in moving quickly and securely to the cloud.
- **We are a member of the AICPA Peer Review Program**, and hold a role on the Colorado Society of Certified Public Accountants.

### Make your compliance programs efficient and empowering with Compliance Essentials

Combining our industry-leading services with the latest SaaS technology, Compliance Essentials is a revolutionary approach to managing compliance activities across more than 40 unique frameworks and is included with our assessment services. Plus, it can lower your total compliance costs by up to 40%.



**Leverage SOC to instill trust in your security posture.**

**Learn more about Coalfire's SOC services.**  
Coalfire.com | 877-224-8077

**C O A L F I R E**

### About Coalfire

The world's leading organizations – including the top five cloud service providers and leaders in financial services, healthcare, and retail – trust Coalfire to elevate their cyber programs and secure the future of their business. Number one in compliance, FedRAMP®, and cloud penetration testing, Coalfire is the world's largest firm dedicated to cybersecurity, providing unparalleled technology-enabled professional and managed services. To learn more, visit [Coalfire.com](https://Coalfire.com).