COALFIRE

DATA SHEET

System Organization Controls report (SOC 1, 2, or 3) advisory services

Meet user expectations by examining and reporting on your controls

A System and Organization Controls report (SOC 1, 2, or 3) is a widely recognized examination to maintain trust and confidence in your organization's security and financial controls performance. SOC reports conform to the guidance prescribed by the American Institute of CPAs (AICPA) Statement on Standards for Attestation Engagements (SSAE).

How Coalfire helps with SOC implementation

We are uniquely qualified and experienced to help you build an internal controls environment that complies with SOC examination requirements. Our methodology starts with assigning dedicated and talented resources based on your organization's industry, services, size, and locations.

Along with assisting you with optimizing timelines and costs during your initial attestation, we evaluate your environment to determine short-term project plans from the perspective of experienced SOC advisors and auditors who maintain the necessary credentials for auditing organizations as prescribed by relevant accredited CPA firm rules.

To determine your organization's preparedness for pursuing formal attestation, our advisors perform a SOC awareness workshop and upfront gap analysis of your applicable in-scope environments by assessing control design and cybersecurity maturity using SOC and technical security expertise. Key objectives and assessment activities include:

- Assisting with identifying and documenting controls.
- Performing control interviews and evidence inspection.
- Determining gaps that require remediation prior to pursing a SOC examination.
- Providing recommendations to address control gaps and security deficiencies.

Establishment

Core document construction

We meet with your governance, risk, and compliance teams to determine the required artifacts related to SOC attestation. Through facilitated discussions with relevant personnel and management, we determine:

- Service commitments and system requirements
- System components used to provide services
- Applicable trust services criteria
- Related controls
- Complementary user entity controls (CUECs)
- Subservice organizations
- Complementary subservice organization controls (CSOCs)

We then draft work products in response to the mandatory requirements for a SOC system description and draft the control inventory for implementation of the in-scope service offering.

Implementation

Policy and procedure development

We augment your organization's internal process owners to establish appropriate policies and procedures that meet security or privacy control objectives within your internal control environment, as appropriate.

Risk assessment

During the risk assessment, we define the objectives within your in-scope system to perform a risk analysis that includes:

- Quantitatively scoring inherent and residual risk based on your risk tolerance scheme.
- Determining risk severity ratings and risk treatment options.
- Developing short-term risk treatment plans for residual risks outside your organization's risk acceptance tolerance based on established criteria.
- Determining each business function's requirements for achieving your security or privacy objectives (e.g., confidentiality, integrity, and availability of information; the overall sensitivity of data supporting these processes).

Key objectives and work products from this phase are a risk analysis worksheet, risk treatment plans, and a risk analysis report.

Internal audit

We execute an independent, periodic internal audit against the security or privacy requirements. As part of the requirements, we inquire, observe, and/or inspect documentation to support your organization's established governance and control procedures. Deliverables include an internal audit plan and report.

Governance review

After the completion of the risk assessment and internal audit inputs, we facilitate the resulting governance review with senior and operations management personnel who are key internal interested parties to the program's establishment. We develop a recurring, supporting agenda presentation template to meet ongoing requirements for this periodic review activity.

External audit support

We help you identify and select an accredited CPA firm that will assess your organization against in-scope requirements. Our advisory team educates you on audit processes and expectations to help prepare you for audit engagements. During the audit, we assist with responding to inquiries related to the advisory work products made by the auditor(s) in interviews and walkthroughs on your organization's behalf. For any identified findings, we assist with management responses and the development of corrective action plans resulting from the external audit.

Effectively prepare for SOC attestation.

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

COALFIRE

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 services, providing unparalleled technology-enabled professional and managed services. To learn more, visit **Coalfire.com**.

DS_SOCAdvisory_051723