

Independent assessments across 100+ frameworks.

Coalfire is one of the industry's leading cybersecurity assessment firms, validating compliance for organizations across cloud, technology, healthcare, financial services, government, and other regulated markets. Twenty-five years, and 3,000 assessments a year.

From a single assessment to a coordinated global compliance program, Coalfire combines specialized assessors, deep framework expertise, and technology to make compliance more efficient and scalable.

Assessment Expertise Across Frameworks

FedRAMP® | PCI DSS | SOC | HITRUST | ISO | Global Compliance | AI

25 Years

Assessing

3000+

Assessment Annually

600+

Framework Experts

100+

Frameworks Supported

Built For More Than A Single Audit

Coalfire supports individual assessments as well as complex, multi-framework programs. Our coordinated approach aligns evidence requests, interviews, testing, and control validation across frameworks to reduce duplicated effort and audit fatigue.

Most companies carry more frameworks than they can assess in a year. We have sequenced enough programs to know which one your business needs now, which can wait a cycle, and which can run together.

Proven Leadership

75%

Of FedRAMP
Authorizations

1000+

PCI DSS
Assessments Annually

500+

SOC Reports Annually

1M+

Combined
Assessment Hours

Why Coalfire

1

Determinations That Hold Up

Any assessor can read a requirement. The harder work is evaluating a compensating control, testing a scope boundary, and deciding whether a finding is material. Those determinations get reviewed by the certifying body, and ours hold.

2

Depth Where It Matters

Dedicated specialists bring deep experience within the frameworks they assess, backed by one of the industry's largest assessment organizations.

3

Scale For Complex Environments

From individual products to enterprise, multi-cloud, and global environments, Coalfire has the capacity and framework coverage to grow with your compliance program.

4

Coordinate, Don't Duplicate

Where requirements overlap, Coalfire coordinates assessment activities across frameworks, reducing repetitive evidence requests, interviews, and testing. Compliance Essentials centralizes that activity, maps requirements across frameworks, and automates portions of evidence collection and review.

When The Framework Requires Testing

Some frameworks require technical testing, not just review. PCI DSS, FedRAMP, HITRUST, SOC, and HIPAA all mandate penetration testing. Coalfire's DivisionHex™, our offensive, defensive, and managed security practice, performs that testing. It also covers what frameworks do not: threat hunting, attack surface monitoring, and AI and ML security testing.

Expertise Beyond The Assessment

When the need extends beyond independent assessment, Coalfire also brings deep expertise in cyber risk and compliance advisory, cloud engineering, and healthcare risk.

ONE PARTNER. CONFIDENCE THAT LASTS.

Let's talk about your compliance goals. Please visit [Coalfire.com](https://coalfire.com)

For more information visit coalfire.com or [contact us](#).