

Risk assurance program

Providing transparency into security risk management

At Coalfire, the security of our customers' information is of paramount importance. Our assessment projects regularly come into contact with sensitive details about your organization, such as policies, procedures, configuration documents, diagrams, and internal security practices. To help build trust, credibility, and assurance that Coalfire is a security-minded partner, we have developed a risk assurance program that provides transparency into our internal security risk management program.

COMPREHENSIVE INFORMATION SECURITY PROGRAM

The information security program surrounding CoalfireOnesm, our proprietary assessment platform, and our broader Coalfire Assessment System (CAS) is regularly audited and examined in accordance with our security testing policy. This policy requires examination of our program annually through an external audit. In February 2018, Coalfire was awarded a SOC Type 1 accreditation by BARR Advisors, with the intent on moving to Type 2 in summer 2018.

Our information security program is based on ISO 27001/2 and NIST 800-53 controls and is governed by our chief information security officer, who regularly reports and communicates program status to the Coalfire Executive Leadership Team (ELT) and Board of Directors. Control implementation is reviewed on an annual basis by external examiners in accordance with our security testing policy.

Security controls program

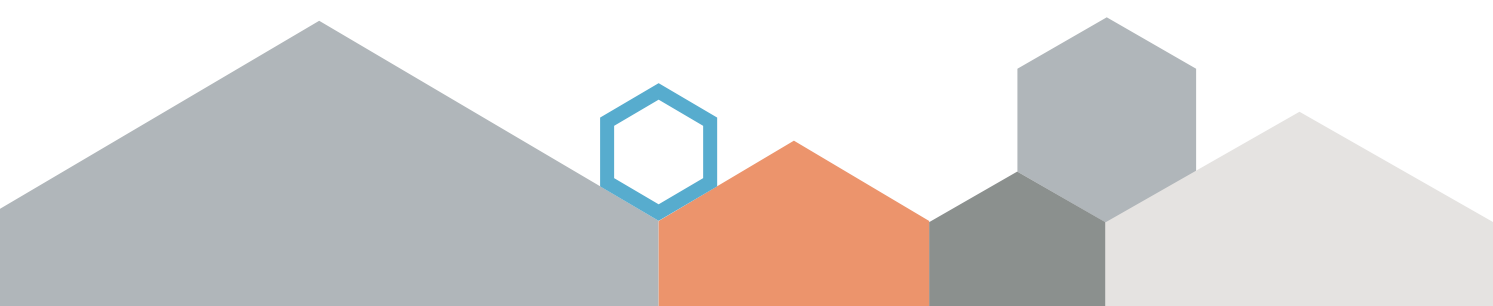
This program addresses physical security, information classification, personnel security, acceptable use, vendor management, and other issue-specific topics. Implementation details are outlined in our documented policies and standards, and relevant areas are published to employees on a need-to-know basis.

IT baseline controls

- **Cryptographic controls:** All "sensitive and proprietary - customer information" is protected via strong cryptography while in transport and storage.
- **IT change management:** All changes to the CAS are documented with key information (i.e., change rationale, backout procedures, potential risks, and implementation procedures) and approved in accordance with a risk-based scale.
- **Systems management:** All systems are managed through a change management database that records problems, system purpose, and status.
- **Network management:** Remote access into the network is controlled through multifactor authentication VPN access to approved users. Additionally, robust monitoring tools identify network-based threats that could signal an intrusion.
- **Security testing:** We examine system and network-based vulnerabilities monthly. Network- and application-level penetration testing is conducted annually. Additionally, an independent auditor reviews our entire program annually, forming the basis of our SOC2 accreditation.

CoalfireOne controls

- **Asset management:** All customer-provided information is stored within Box for Government, which includes Box Governance, Box Zones, and Box KeySafe layered on top of Box Enterprise. No data is exposed to Box or Box employees due to the self-controlled, AES-256 encrypted Coalfire keys managed in AWS GovCloud.
- **Software development lifecycle:** We observe a written, agile-based development lifecycle process that governs all stages of the CoalfireOne environment.
- **Web application firewall:** All inbound and outbound traffic to CoalfireOne is mitigated through the use of AWS Web Application Firewall and Elastic Load Balancing.
- **File integrity monitoring:** CoalfireOne servers are continuously monitored for changes to critical system processes and files. Suspicious events are escalated to Coalfire security.
- **AWS VPC Traffic IDS:** Network traffic to and from sensitive servers are examined for suspicious activities that could indicate hostile activities.
- **Encryption:** All traffic to CoalfireOne is protected through the use of TLS 1.2 using AES-128 and AES-256 ciphers. All information stored in Box is encrypted using AES-256 encryption.
- **Multifactor authentication (MFA):** MFA can be implemented on the CoalfireOne organizational account and applies to all organizational users. Customer MFA uses Google Authenticator to generate a one-time code that must be supplied with the user password. All Coalfire users must use MFA when accessing CoalfireOne from a remote network.
- **Incident management:** We maintain a documented incident response plan (IRP) that establishes the processes our organization observes when escalating a security event into an incident, as well as the subsequent processes that must be observed to investigate, contain, eradicate, and recover from the incident.



UNDERSTAND THE CONTROLS
WE'VE IMPLEMENTED TO PROTECT
YOUR INFORMATION THROUGHOUT
YOUR ASSESSMENT.

Download our risk assurance program
white paper at [Coalfire.com/Risk-Assurance-Program](https://www.coalfire.com/Risk-Assurance-Program)
Coalfire.com | 877.224.8077

CALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 17 years and has offices throughout the United States and Europe. [Coalfire.com](https://www.coalfire.com)