COALFIRE

Data Sheet

FedRAMP® 3PAO Assessment Services

Expertise and technology to get assessment-ready in less than six months

FedRAMP authorization can open up significant market opportunities, but achieving a FedRAMP ATO can be challenging, costly, and time-consuming due to the rigorous security standards and extensive documentation required. Coalfire®, a FedRAMP Third Party Assessment Organization (3PAO) leader, provides expert-led services, including security control assessments, vulnerability scans, and penetration testing to help cloud service providers (CSPs) successfully expand into federal markets.

FedRAMP Readiness Assessment

The Coalfire assessment team thoroughly reviews the authorization boundary to ensure accurate representation of all external services, interconnections, and data flows.

This process includes the validation of federal mandates and requirements, along with the definition of capability information within the Readiness Assessment Report (RAR) template. The RAR consists of a detailed executive summary highlighting notable strengths and weaknesses, control implementations, and the overall maturity of the information system.

FedRAMP Initial Assessment

The Coalfire assessment team creates a Security Assessment Plan (SAP) that outlines details for conducting the assessment and the timeline for key milestones.

It covers all baseline security controls for the system's security impact level. The assessment includes technical interviews to validate control implementations and identify any risks discovered through manual control testing, vulnerability scanning, and penetration testing.

The team produces a comprehensive Security Assessment Report (SAR) that details any identified risks, the impact of these risks on the information system, and the necessary remediation activities to reduce or mitigate the risks.

Submission to Obtain an ATO

The Coalfire team performs all testing in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

Coalfire captures the results in a SAR. Once the SAR is complete, Coalfire submits it to the agency sponsor and the FedRAMP Program Management Office (PMO) for their review and to obtain an ATO. Throughout the sponsor and PMO package review process, the reviewer requests additional information to clarify testing activities, remediation steps, and insights on any gaps noted.

FedRAMP Annual Assessment

Coalfire assists in preparing the annual assessment before the ATO deadline. The annual assessment process includes the assessment of approximately one-third of the required security controls, plus any additional controls required by the agency sponsor or FedRAMP PMO. The assessment performs manual control testing, vulnerability scanning, and penetration testing.

Maintaining an ATO

To maintain a FedRAMP ATO, a CSP should monitor the security control environment, assess regularly, and demonstrate that the service offering's security posture is continuously acceptable. Ongoing assessment to maintain authorization provides federal agencies using cloud services with a method for detecting changes to the system's security posture and making risk-based decisions.

Additional Federal Assessments

Coalfire can help you with the following assessments as individual assessments or in tandem with FedRAMP assessments:

- **Department of Defense Risk Management Framework (DoD RMF):** Our DoD RMF certification and accreditation service assesses your information systems to DoD RMF standards.
- **NIST SP 800-53 assessment:** Assess, test, and review your information systems with our in-depth testing and assessment capabilities.
- **International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR):** Our ITAR and EAR assessment services help you navigate the cybersecurity aspect of the export control compliance process.
- **NIST SP 800-171 assessment:** We provide assessment services to help compliance process for the FAR (Federal Acquisition Regulation) and DFARS (Defense Federal Acquisition Regulation Supplement) cybersecurity contract obligations. We also assess security controls and contract obligation compliance and ensure continuous compliance monitoring for providers that store, process and transmit Controlled Unclassified Information (CUI).
- **Drug Enforcement Administration (DEA) Electronic Prescriptions for Controlled Substances (EPCS):** Every two years, providers and pharmacies must undergo a third-party audit of their electronic prescription or pharmacy management applications to achieve DEA EPCS certification. Rely on our auditing program for your EPCS assessment and certification.

FedRAMP Pen Testing

Coalfire leads the industry in cybersecurity by excelling in both FedRAMP penetration testing of all six attack vectors (external to corporate, external to CSP target system, tenant to CSP management system, tenant to tenant, mobile application to target system, and client-side application or agents to target system) and in the advanced red team assessments now required by FedRAMP Revision 5.

We are renowned for our expertise, allowing us to rigorously evaluate and strengthen systems against many potential vulnerabilities and meet stringent FedRAMP standards.

Why Coalfire?

Compliance Capabilities Leader

Coalfire's FedRAMP-certified auditors and penetration testers work with hundreds of major cloud service providers and contribute to 3PAO Special Interest Group, FedRAMP PMO initiatives, and ACT-IAC FedRAMP working group.

Tailored Delivery Experience

Coalfire experts are dedicated specialists in specific frameworks, ensuring tailored solutions for each client. They understand the entirety of the client's business and function as strategic partners rather than just one-time vendors. 75% of all FedRAMP authorizations are managed by Coalfire.

Compliance Essentials Platform

Our compliance automation solution, Compliance Essentials, is a SaaS platform that supports over 75 frameworks. Compliance Essentials helps organizations implement coordinated assessments to eliminate duplication of efforts.

For more information visit **coalfire.com/fedramp-assessment-services** or **contact us.**

Copyright © 2024 Coalfire Systems, Inc. All rights reserved. Coalfire, the Coalfire Logo, CoalfireOne, the Coalfire|Talks Logo, the Hexagon Logo, Hexeon, Neuralys, RAMP/pak, RAMP/pak+, RAMPcon, the RAMPcon Logo, and ThreadFix are trademarks or registered trademarks of Coalfire Systems, Inc. or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.