

AI Risk Management Services

Manage AI risk from threat actors and quickly evolving regulations

Most organizations cannot ignore the significant competitive advantages and efficiency gains recognized from AI adoption. As with many new technological innovations, AI can create risks that expose organizations to threat actors and rapidly changing regulations. Coalfire offers a portfolio of cyber security services to help you manage the risks that AI can introduce. Coalfire AI governance and compliance services can help your organization navigate the risk and compliance challenges related to AI development, adoption, and integration into business models and processes.

AI Solutions Tailored to Unique Organizational Needs

Recognizing that AI adoption is a journey, and some organizations are just getting started while others are further along, the Coalfire AI offerings seamlessly integrate into each phase of the AI information system lifecycle. Whether your organization is designing systems, implementing AI solutions, or subject to formal evaluations, Coalfire services complement and enhance the AI product lifecycle and associated compliance obligations.

AI Risk Workshop and Governance Strategy

The National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) provides a comprehensive set of standards and best practices to assist individuals, organizations, and societies in identifying and managing risks associated with AI development. Based on the NIST AI RMF, Coalfire's AI risk assessment identifies potential AI system development and usage threats and vulnerabilities. Coalfire assesses your security program's defense of AI systems and provides detailed recommendations to better secure system access, minimize data disclosure risks, and address privacy/bias concerns.

AI Risk Program Build

Coalfire will advise and develop AI governance documentation, identify and map AI risks, and develop risk remediation plans aligned with emerging frameworks and guidance from regulatory and international standard bodies.

Threat Modeling and Security Evaluation

Threat actors see AI implementations as a potential new attack surface. Coalfire will provide a comprehensive risk analysis of an organization's (machine learning) ML models, including Large Language Models (LLMs), adhering to established standards such as OWASP. The evaluation identifies potential threats and determines model weaknesses against adversarial attacks through technical testing and threat modeling to provide practical recommendations to improve the security of the model and its interactions within its operating environment.

Penetration Testing

Coalfire performs a comprehensive evaluation of the infrastructure that supports your organization's AI models with the Coalfire Infrastructure Security Assessment service. This service thoroughly examines network, cloud, API security, and other critical areas using AI pen testing and red teaming. Coalfire cyber security services will rigorously examine applications incorporating LLMs and other machine learning elements, ensuring they are fortified against vulnerabilities and function reliably under various conditions, including adversarial threats. Coalfire will help ensure the organization's deployment of AI is robust, adheres to multi-layered defense strategies, and minimizes risks.

AI Compliance Readiness

Coalfire performs a comprehensive gap analysis against key regulations, standards, and frameworks to identify design and implementation gaps in your AI governance program. Frameworks in the readiness program include but are not limited to:

- **ISO/IEC 42001:2023: Artificial Intelligence Management System**
- **HITRUST v11.2**
- **NIST Artificial Intelligence Risk Management Framework (NIST AI RMF)**
- **Criteria Catalogue for AI Cloud Services (AIC4)**
- **EU Artificial Intelligence Act**

AI Governance Attestation

Upon successful completion, Coalfire will issue a formal attestation of your organization's AI program, confirming that your organization has taken appropriate steps to manage its AI risk.

Coalfire AI Services

Aligned to the NIST AI RMF, Coalfire provides a comprehensive suite of services to design, execute, manage, and operationalize your AI Risk Management program.

- **AI Risk Workshop & Governance Strategy**
- **AI Risk Program Build**
- **Threat Modeling**
- **Penetration Test**
- **AI Compliance Readiness**
- **AI Governance Attestation**

Coalfire has extensive expertise and experience related to AI and ML system security. As cybersecurity thought leaders, Coalfire is at the forefront of AI security, demonstrating our expertise through participation in podcasts and webcasts, actively participating and serving as a lead contributor to OWASP's Top 10 for ML Applications guidance, as well as contributing to the development of the Cloud Security Alliance (CSA) security guidelines for AI. Additionally, we engage in collaborative research with top universities to develop cutting-edge AI security techniques. Our experts engage deeply with clients to create bespoke security strategies that ensure AI and ML implementations are secure, compliant, and ethically sound.

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