COALFIRE

DATA SHEET

Artificial intelligence risk management

Effectively respond to rapidly changing technology with expert leadership and assurance services

Artificial intelligence (AI) technology fosters the development of machines or applications to perform tasks that usually require humans. While AI is not new, the eruption of massive mega data collection, affordable high-speed cloud computing, and decreasing data storage and computing costs have brought AI into the epicenter of application development to support critical business operations. However, the recent rush to leverage this longstanding technology has created a regulatory and cybersecurity vacuum that could leave your business at risk.

How do AI risks differ from other software risks?

AI-based technology poses risks and challenges that do not strictly fall under a traditional cybersecurity program. Before adopting AI, your company should consider the security and ethical dangers associated with AI, including:

- Legal, regulatory, and privacy concerns
- The possibility of misinformation, manipulation, and unexpected behaviors
- Societal bias and discrimination
- Job displacement
- An overreliance on AI

Our approach

Coalfire's AI experts provide tools and assistance to help you evaluate and contain AI risk across your organization. Our AI assessment approach, leveraging the NIST AI 100-1 Artificial Intelligence Risk Management Framework, can help you understand and address the risks and impacts associated with AI product development while optimizing the potential benefits of AI technology.

We work with your team to set maturity goals and assess the key functional areas of your AI technology development program:

- **Govern:** Evaluate the implementation of a risk management culture within your organization's design, development, deployment, evaluation, or acquisition of AI applications and systems.
- **Map:** Examine the AI lifecycle and the interdependent activities associated with the product development cycle that is used to manage the appropriateness and use of AI solutions.
- **Measure:** Assess quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts.
- **Manage:** Categorize risk resource allocation, implementation, and functional effectiveness to ensure that risks are prioritized and acted upon based on projected impact.

Our AI risk assessment methodology is built on a best-practice approach for satisfying regulatory requirements. We document known risks and seek to uncover new risks, so your organization can build a comprehensive and more mature security program. Our methodology includes:

- Scope determination
- Data collection approach
- Identification of potential threats and vulnerabilities
  - Assessing current security measures
  - Determining the impact of threats and your level of maturity
  - Finalizing documentation

Deliverables

After the assessment, we deliver an executive-level report that summarizes your organization's potential risks and proposed remediation actions. We also provide a detailed worksheet on identified risks, potential impacts, implemented controls, and risk mitigation recommendations.

AI risk advisory

To help you navigate the changing AI regulatory landscape, our experts can assist with remediating identified gaps or provide ongoing guidance on security risk management of AI technology. Our knowledgeable consultants offer advisory services that can help you follow best practices and properly address the unique risks associated with AI technology.

Why Coalfire

- Our experts have multiple security-related certifications, including CISSP and CRISC, and have built and implemented programs that adapt to new technologies and changing security threats.
- Leveraging our deep understanding of the risks facing organizations today, we partner with you to establish and maintain a programmatic cybersecurity risk management approach that matches your business's operations.
- Our experience working with numerous commercial and government clients gives us a deep understanding of data complexity, enabling us to assess sensitive data in the most thorough and comprehensive manner in all environments.
- The information provided through our risk assessment can help you proactively acquire an adequate budget from your leadership team.

Securely leverage AI technology.

Learn more about our AI risk management 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 technologyenabled professional and managed services. To learn more, visit **Coalfire.com**.

DS_AIRiskManagement_112722023