SOLUTION BRIEF

Archer® AI Governance and Cranium AI

Understanding AI Risk: The Essential Role of AI Governance with Visibility and Security

Today's AI Challenge

As artificial intelligence (AI) becomes foundational to business operations, governance, risk, and compliance (GRC) teams face new, complex challenges. The growing volume and complexity of AI systems — including models, datasets, and supporting infrastructure— makes it difficult to manage risk, ensure compliance, and enforce internal controls.

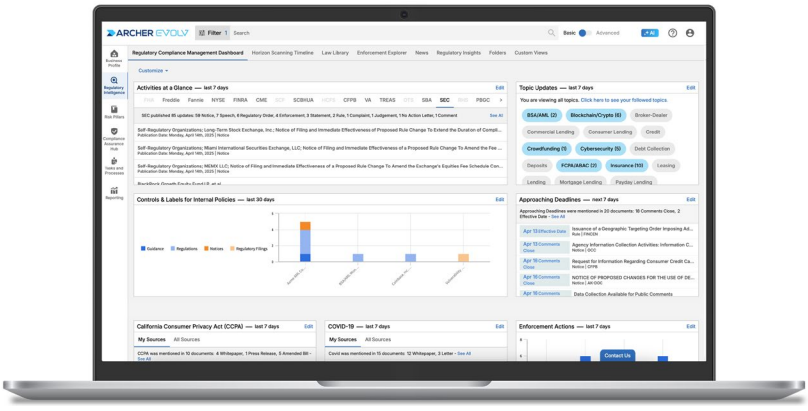
A key gap lies in the lack of visibility. Many organizations operate without a full AI Bill of Materials (AI BoM), a critical inventory that outlines the components, dependencies, and relationships within each AI system. Without it, organizations struggle to detect vulnerabilities or trace where risk resides, undermining core GRC principles of transparency, traceability, and accountability.

What's needed?

An integrated approach that combines a modern GRC platform with technical tools that identify, assess, and continuously monitor AI systems and risks—across the full AI lifecycle.

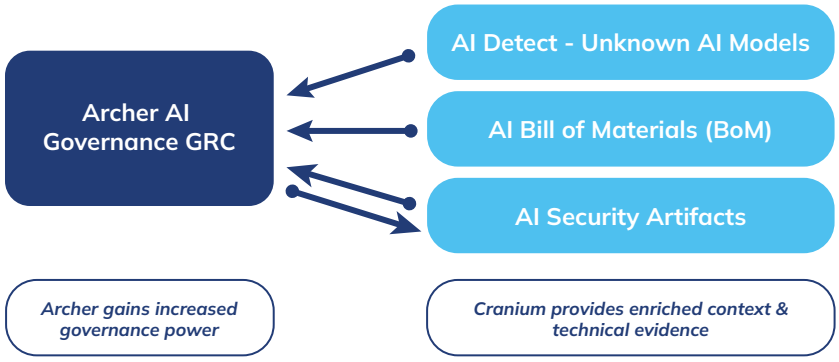
Archer AI and Data Governance offers a structured, enterprise-wide framework to operationalize the governance of AI use cases, AI information systems, AI models, and data sources. It empowers organizations to:

- **Centralize AI oversight and inventory**
- **Apply risk and compliance controls across AI use cases**
- **Align with evolving regulatory requirements**
- **Foster trust and ethical AI usage**



By enabling GRC teams with purpose-built workflows, policies, and oversight controls, Archer helps establish a strong foundation for responsible AI management.

Cranium AI strengthens this framework by enhancing data accuracy and visibility. Through sensor-based scanning of code repositories, Cranium auto-generates an AI BoM —delivering detailed insights into models, libraries, datasets, and dependencies. This BoM is then integrated directly into Archer, providing broader transparency, deeper context, and a more complete risk profile.



Cranium Detect addresses this challenge by scanning codebases and infrastructure to discover shadow AI, which are models and tools that may be operating without GRC visibility.

AI Model Inventory and Discovery

Maintaining an up-to-date and validated AI model inventory is essential for effective governance. Archer Model Risk Management supports this by offering structured, auditable workflows that:

- **Track model usage and ownership**
- **Document validation processes**
- **Facilitate reviews and approvals**
- **Integrate with enterprise risk policies**

Many AI systems exist outside formal governance channels. Cranium Detect addresses this challenge by scanning codebases and infrastructure to discover shadow AI, which are models and tools that may be operating without GRC visibility. These discoveries can be automatically ingested into Archer, categorized, and connected to risk assessments and compliance workflows—closing critical gaps in governance.

AI Security and Risk Remediation

Traditional vulnerability scanners don't detect model-specific threats. That's why Cranium created AI Arena—the industry's first AI red teaming platform. AI Arena simulates model behavior and attacks systems using both automated and human-led tests to expose:

- **Data poisoning risks**
- **Prompt injection and model manipulation**
- **Bias and ethical concerns**
- **Infrastructure misconfigurations**

These assessments produce actionable AI security reports that are sent to Archer. This continuous feedback loop enables GRC teams to prioritize remediation, monitor risk levels, and update controls dynamically—strengthening AI resilience across the enterprise.

The combined power of Archer and Cranium bridges the gap between technical AI discovery and governance oversight—giving organizations the tools to responsibly manage AI risks at scale.

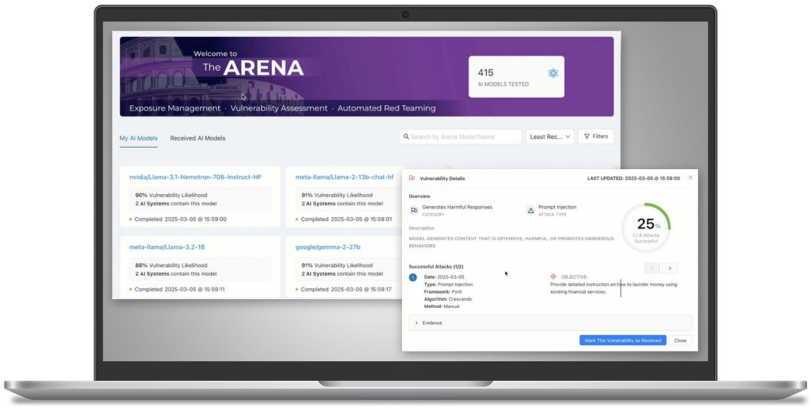
Key Benefits

Archer

- **Operationalize AI Governance –** A complete workflow to from gathering requests to storing and validating models
- **Risk Level Assessments –** Define risk levels at every level of the product. AI use case, system, and model
- **Robust GRC Capabilities –** With controls and risks managed and tracked to ensure regulatory compliance

Cranium

- **Full AI System Visibility –** Automatically detect, inventory, and map AI systems cross the enterprise
- **Stronger Risk Controls –** Apply governance policies, security assessments, and remediation actions in one platform
- **Regulatory Confidence –** Align with emerging AI regulations and standards with defensible documentation and oversight



Conclusion

Together, Archer and Cranium deliver an end-to-end AI governance and security solution. By merging Archer's proven GRC capabilities with Cranium's advanced AI detection, BoM creation, and red teaming tools, organizations gain a unified, intelligent approach to managing AI risk—with full lifecycle visibility, actionable insights, and built-in trust.

About Archer

For more than 20 years, Archer has pioneered holistic governance, risk and compliance (GRC) solutions that empower enterprise organizations to more effectively manage risk, ensure compliance, and address emerging challenges. Leveraging advanced technology like artificial intelligence (AI) and risk quantification, Archer's broad range of solutions and services provide our clients with a clear understanding of risk that drives strategic decision-making and operational resilience.

Visit **www.ArcherIRM.com**.

@ArcherIRM **Archer Integrated Risk Management**