LevelBlue

SOLUTION BRIEF

AI Cyber Risk Management

A Blueprint for Safeguarding Your Organization

A Blueprint for Safeguarding Your Organization

Organizations are progressively moving towards integrating Artificial Intelligence (AI) into their operations. This is driven by the assurance of AI to revolutionize processes, enhance decision-making, and unlock new opportunities for innovation and efficiency. As a result, the demand for AI technologies is increasing. However, as AI tools become more affordable and widely available, their cybersecurity risks are also increasing. Many organizations are adopting AI technologies without fully accounting for the potential security and privacy implications. Beyond that, there are a myriad of regulations that have passed or are on the horizon.

Understanding the Security Risks of AI

One of the main challenges organizations face with this adoption is the sophistication of cyberthreats. AI is creating more advanced malware and phishing attacks that are harder to detect. Additionally, the AI models can become targets, with the potential for theft, alteration, or corruption, posing additional threats to the organizations. Data privacy is another significant challenge, as AI systems have access to vast amounts of data, raising the risk of protecting sensitive information.

Rather than only reactively mitigating risk, deliberate deployments of AI should primarily serve a detailed purpose. All deviations can be monitored in the context of missing that original purpose or slowly deviating from it—such as data and model drift—leading to unintended outcomes.

Importance of AI Risk Management

AI risk management can help organizations ensure that AI is used responsibly and ethically. A strong AI risk management strategy allows businesses to identify, assess, and address potential threats, ensuring the secure and responsible deployment and use of AI technologies. This protects the organization from disruptions and legal issues, and builds trust with customers and stakeholders. Additionally, AI risk management enables businesses to make informed decisions, balancing innovation with risk and maximizing the benefits of AI technologies.

Benefits

Organizations that partner with LevelBlue can expect:

- Establish guardrails to ensure responsible use of AI.
- Enhance trust and credibility among users, stakeholders, and regulators.
- Reduced risk of data breaches and associated costs.
- Early identification of potential ethical, legal, operational, and reputational risks.
- Enabling AI applications compliance with current laws and standards, helping to avoid legal penalties and fines.
- Optimize AI performance by identifying potential security risks to ensure they operate efficiently and effectively.
- Evaluations and management that AI technologies are being used responsibly.

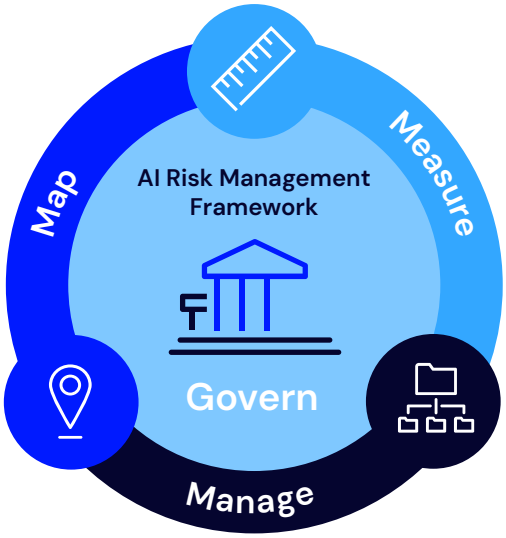
Also, without a well-planned strategy to manage risks and issues, AI initiatives will deteriorate over time. AI models and systems will lack integrity without a foundational commitment to fairness and ethics. Thus, considerations of these elements cannot be secondary; they must be integral. IT leaders need to proactively identify these risks and determine the balance between the overarching risks of AI and the advantages its implementation brings. Organizations can manage and mitigate the risks associated with AI by conducting an AI Cyber Governance and Risk Management Assessment.

LevelBlue AI Cyber Governance and Risk Management Assessment

LevelBlue's AI Cyber Governance and Risk Management Assessment is a comprehensive evaluation, essential for organizations of all sizes and industries considering integrating AI into their operations. This assessment serves as the foundation for implementing effective governance and establishing the processes for identifying and addressing security risks within AI systems and their deployment, ensuring that cybersecurity measures are robust and current. Establishing AI governance is a crucial step for organizations to ensure that their AI systems are ethical, transparent, and in compliance with regulations, while also maximizing their effectiveness and minimizing risks.

LevelBlue will determine the readiness to integrate AI in a structured governance and risk management framework that outlines how decisions are made regarding AI projects. This framework should include policies, standards, and guidelines for developing, deploying, and ongoing management of AI systems.

This would entail setting governance objectives, establishing a multidisciplinary team, having risk assessment methodologies in place for AI, managing risks identified, establishing continuous monitoring and reporting, and reviewing and adapting governance processes.

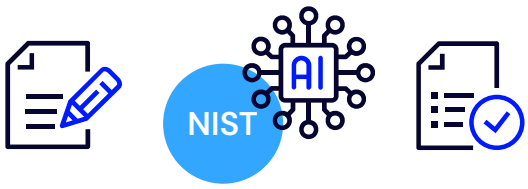


Through Our AI Cyber Governance and Risk Management Services, We Assist Organizations to:

- Identify gaps related to AI in their cybersecurity and risk management programs
- Prepare for regulatory requirements and establish and improve security related to AI, providing due diligence to third parties and auditors
- Document findings and provide recommendations to establish a roadmap to integrate AI in the security governance and risk management program and product/system lifecycle

How Does LevelBlue Perform an AI Cyber Governance and Risk Management Assessment?

LevelBlue's AI Cyber Governance and Risk Management Assessment is a comprehensive assessment of your organization's preparedness to manage and mitigate risks associated with the deployment and use of AI technologies. Our approach is based on industry frameworks, like the NIST AI Risk Management Framework (NIST AI RMF).



Risk Management Framework

OUR LEVELBLUE TEAM OF EXPERTS WILL UTILIZE THE APPROACH SUMMARIZED BELOW:

ASSESSMENT

Preparation and Planning	Work to prepare and plan the kickoff meeting, assessment activities, key stakeholders, and project timing.
Information Gathering	Understand existing cyber governance and risk management practices, the current state of cybersecurity and foundation to easily adopt or develop AI, roles, and responsibilities across the organization involved in the governance, adoption, and development of AI, and AI use cases.
Review and Analyze	Evaluate current governance and risk management practices to compare to the NIST AI RMF and practices established within the industry for adopting, using, and developing AI.
Reporting and Recommendations	Develop prioritized recommendations for a strong governance and risk management structure for responsible AI.

Why LevelBlue?

LevelBlue offers expertise and specialized knowledge that is critical for identifying and mitigating the risks AI presents. Our team can provide a customized mitigation strategy tailored to your organization's specific needs and objectives—enhancing operational efficiency and safeguarding against potential threats. Additionally, working with LevelBlue helps organizations to stay ahead of regulatory compliance and maintain stakeholder trust by demonstrating a commitment to cybersecurity.

For more information, visit LevelBlue.com

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.