NOPALCYBER

eBook

AI IS IN YOUR ENVIRONMENT. IS IT UNDER YOUR CONTROL?

info@nopalcyber.com | 917.512.4489

www.nopalcyber.com

AI Is in Your Environment. Is It Under Your Control?

With so much enthusiasm around AI, along with so much expectation to accelerate adoption, it would be easy to focus entirely on the upsides. However, the same characteristics that make AI so rewarding also make it risky to an equal or greater degree. Few tools can accomplish as much as artificial intelligence. Few tools can do as much damage, either.

- **Cyber attacks are the most obvious risk**, and there are a growing number of examples of AI tools being weaponized to steal data, break systems, and empower bad actors. Malicious prompt injection attacks rose by 32% just between November 2025 and February 2026.
- **AI misuse opens the door to lawsuits, compliance violations, and angry customers**, all of which can damage a company's reputation and revenue. In one survey, 44% of Gen Z workers admit to intentionally sabotaging company AI.
- **Bias and hallucinations may result in important decisions based on bad information.** Legal research created with AI has been shown to create nonexistent quotes and citations.
- **Costs are another concern**; as the price and prevalence of AI both skyrocket, huge bills might appear unexpectedly. Companies spent 19% more for cloud computing in 2025 alone, and AI is quickly becoming the largest IT line item.

Any one of these risks would pose a serious setback. Together, they could spell disaster for any company on earth.

As we accelerate into the AI era, adopting the right mindset and strategy becomes just as important as picking the best vendors and use cases. More than just a new technology,

AI represents a revolution in risk.
It can hurt just as much as it can help.

Companies need to take AI governance *very seriously* starting immediately. It must be a core component of any AI strategy, whether it's still taking shape or already underway. In the balance of risk and reward, AI governance is the fulcrum, positioned in the middle and determining whether things tilt in a positive or negative direction.

This ebook explains why everything depends on AI governance, then outlines a model any company can follow to get governance right.

What Makes AI Different From Other Technology?

AI is unlike any technology that came before it. Beyond the unique risks and rewards, the fundamental characteristics of AI make governance both extremely important and uniquely difficult:

Autonomous

AI works independently to complete whatever task it was assigned, making autonomous decisions about the most efficient and effective way to proceed. Since a person isn't controlling what the AI does, it's essential to have guardrails and safety measures in place to prevent the AI from causing any harm. **AI does what it wants.**

Instantaneous

AI makes countless decisions in real-time at a pace much faster than any human thought process. Governance frameworks are typically based on periodic reviews and manageable speeds, but AI moves so quickly across so many domains that it causes governance to accelerate or lag behind. **AI works at warp speed.**

Probabilistic

Most technologies are deterministic, meaning they work in a consistent, predictable way, but AI is probabilistic, so it follows unpredictable patterns. Any system where the rules and results are always changing will need to have visibility and controls built in to avoid unwanted results. **AI doesn't follow a consistent playbook.**

Evolving

Massive sums of money are being spent to advance AI capabilities, leading to huge strides in a short time and suggesting that AI will evolve rapidly in the years to come. Any effort at AI governance will need to evolve just as quickly to keep pace with the applications, risk exposure, and threat landscape. **AI is changing constantly.**

Opaque

Many AI models work in a "black box" fashion where it's uncertain why and how they gave a certain answer or pursued a specific course of action. When users can't see inside a solution to understand how it works, they must work to make these solutions as transparent and auditable as possible to ensure accountability. **AI is hard to see inside**.

Integrated

AI, particularly agentic AI, will interact with many different systems and data sources and rely on widespread access privileges to complete a given task. That makes it especially dangerous if the AI were to malfunction or get hijacked because it could cause problems that spread across a whole company or beyond. **AI touches the entire infrastructure.**

The Reality of AI Risk

77 AI-related incidents happened in 2021 compared to 320 in 2025.
(source)

500% increase in AI-generated email attacks in 2025.
(source)

97% of leaders expect AI agents to cause a security incident in the next 12 months.
(source)

78% of executives think their company would fail an AI governance audit.
(source)

Understanding AI Governance

"Traditional GRC tools are simply not equipped to handle the unique risks of AI, from real-time decision automation to the threat of bias and misuse." (source)

LAUREN KORNUTICK, GARTNER

In the same way that AI breaks the mold of all previous technologies, it requires new ways of thinking about governance. Traditionally, governance has been used to manage risk, preserve compliance, uphold ethics, and keep a company stable. AI turbocharges all those imperatives, making each one more complicated, fast-moving, and high-stakes than before. The only way to mitigate all the damage that AI could cause, while maximizing all the advantages it has to offer, is through a sustained and serious focus on AI governance.

In practice, governance will involve creating, evaluating, enforcing, and updating policies around acceptable AI usage. Those policies will define everything from what AI tools are acceptable to use, which use cases are approved or prohibited, how data is stored and secured, who is authorized to make decisions and changes, and myriad other considerations.

The specifics will reflect a company's tech stack, AI dependence, risk profile, size and industry, corporate strategy, and more, but compliance mandates will have the biggest influence. AI regulations are evolving quickly—most world powers have either proposed or approved rules—and one day companies will need to comply with a patchwork of state, federal, and international requirements. Looking at the guidance already in place reveals what AI governance will need to address:

NIST AI RMF

This voluntary standard is quickly becoming the best practice in the absence of more explicit AI regulations. It covers four functions—govern AI, map risk, measure impact, and manage response—and is designed to be a flexible playbook that companies can align with their own plans and priorities.

ISO/IEC 42001

This international standard specifies how to reduce AI risks through a managerial approach based on four pillars: organizational governance, risk management, ethical principles, and continuous improvement. Unlike the NIST framework, ISO 42001 alignment can be certified by a third-party auditor, thus proving a company takes AI governance seriously.

EU AI Act

The world's first (but certainly not last) comprehensive AI law was passed in June 2024 and separates AI usage into three categories: unacceptable risks that must be avoided, high risks subject to assessment and accountability requirements, and transparency requirements that apply to almost all AI applications.

Neither the US nor India has passed federal regulations around AI, but they have published proposals that could one day become laws. While vague, both in terms of what's required and how penalties will work, these and similar documents from other governments suggest that AI regulations will take effect sometime soon.

Until then, aligning with one, or ideally all, of the standards outlined above creates a strong foundation for AI governance and a shortcut to future compliance.

The Five Pillars of AI Governance

Ethics

Review the ethical implications of every AI initiative during planning, testing, and deployment.

Risk Management

Classify AI application risk as low, medium, or high, then govern accordingly.

Transparency

Document the training data, decision logic, and performance metrics for all AI.

Accountability

Define who owns, monitors, manages, and takes responsibility for each project.

Compliance

Identify all applicable regulations, their requirements, and any rule changes.

A Sustainable Solution for AI Governance

AI is the catalyst for a governance shift, but it's having a similar effect on strategy, markets, and entire industries, all while the world economy undergoes a series of system shocks. Which is to say, companies must become experts in AI governance while also pouring significant resources into adapting, evolving, and competing in a time of disruption.

In order to balance AI governance with many other competing priorities, companies should enlist outside assistance. Governance experts help clients evaluate risks and requirements, plan and implement governance programs, and assess and improve effectiveness over time. In addition to taking this burden off of internal teams, outside partners ensure that governance is as thorough, efficient, and compliant as possible so that companies can take full advantage of the AI revolution.

Nopal Cyber offers AI governance assistance to diverse companies, including those in high-risk and high-compliance industries like legal, finance, and healthcare. Our services include:

- AI compliance readiness assessments
- NIST AI RMF implementation
- ISO 42001 readiness programs
- EU AI Act gap analysis
- AI governance framework design
- A range of services to secure AI

Governance is the cornerstone of any AI strategy and the single greatest driver of success. We make it accessible to all, effective for everyone, and compliant in all contexts. Rely on our expertise to get AI governance off the ground. Then turn to NopalCyber to help scale, assess, and evolve governance over time. The work pays massive dividends.

Start a conversation with our team.

Contact NopalCyber

NOPALCYBER

The security of knowing you're secure.

www.nopalcyber.com

info@nopalcyber.com

About NopalCyber

NopalCyber makes cybersecurity manageable, affordable and reliable. Managed extended detection and response (MXDR), attack surface management (ASM), breach and attack simulation (BAS), and advisory services fortify your offensive and defensive cybersecurity posture. AI-driven intelligence in its Nopal360° platform, the NopalGo application, and its proprietary Cyber Intelligence Quotient (CIQ) lets anyone quantify, track, and visualize their cybersecurity posture in real-time. NopalCyber's offensive and defensive services and external threat analysis are tailored to each client's need. NopalCyber democratizes cybersecurity by making enterprise-grade security available to organizations of all sizes.