

# Why an Enterprise AI Governance Strategy Should Top Your To-Do List

By **Renaud Baguena, Todd Cherkasky and Sucharita Venkatesh** • July 10, 2025



**Renaud Baguena**

Group Vice President,  
Global Head of Risk  
Management



**Todd Cherkasky**

GVP Customer  
Experience &  
Innovation Consulting,  
Publicis Sapient,  
Chicago, IL



**Sucharita Venkatesh**

Senior Director General  
Management, Publicis  
Sapient, London,  
United Kingdom



Artificial Intelligence (AI) is no longer the stuff of science fiction—it's already firmly embedded in our business world, transforming how we work, think and compete. From making quicker decisions to optimizing operations, AI is helping businesses not just keep up but get ahead.


But there's a catch. While AI is opening the door to a world of possibilities, it's also introducing its own set of challenges. Chief among them: the need for governance, a framework that lays out the ground rules of your organization's AI use.

This guide is designed to help business and technical leaders understand and implement effective AI governance, safeguarding their organizations against risks while maximizing the benefits of AI. But it's not just about reducing risk—it's about building integrity and trust into AI operations and designing a better solution for all stakeholders. That's why getting AI governance right isn't an option; it's a necessity.

# What is AI governance?

Running AI without governance is like playing a high-stakes game without a rule book or a referee. It's only a matter of time before it goes off the rails. That's where AI governance comes in. It establishes a reliable framework, ensuring AI technologies are aligned with ethical standards, regulatory requirements, business objectives and consumer expectations.

Think of AI governance as an operating manual or rule book—your organization's playbook that lays out the who, what and how of AI's ethical and legal use. It's about building a strong foundation of trust and integrity into your AI system, so it not only does what you want but does it in a way that complies with laws and social norms. And without a robust governance framework, your organization risks making a misstep that could lead to disastrous consequences, such as privacy violations, reputational harm, legal sanctions and financial losses.

Air Canada learned that: After the company's AI-powered chatbot [mistakenly told a customer that he could get reimbursed](#)  after purchasing a bereavement fare, the airline refused to honor it. The customer took out a claim against Air Canada. The case resulted in negative publicity for the company, which was also ordered to pay damages.

AI governance has a simple goal: ensuring the responsible, ethical and legal use of AI. To do this, it brings together several key principles that make sure your AI systems don't just work but do so with integrity and accountability. Those principles include:

**Transparency:** This is the streak-free window into your AI processes. AI systems are designed to be understandable and their decisions traceable by stakeholders. Transparency is crucial in sectors like banking, where decisions on loan approvals must be clear to both regulators and customers to ensure fairness and prevent discrimination.

**Fairness:** AI systems can inadvertently encode biases present in the data they are trained on, leading to unfair outcomes. For example, an AI system designed for hiring might prioritize candidates from certain demographics if not properly vetted for bias. Thus, fairness involves deploying strategies to identify, minimize and eliminate these biases, which can include diversifying training datasets and regularly auditing AI outcomes.

**Accountability:** Defining clear lines of responsibility for AI processes is critical for

maintaining accountability. This includes having designated roles such as AI project managers or chief AI officers (CAIO) who are tasked with ensuring that AI deployments adhere to ethical guidelines and achieve intended business outcomes without unintended negative consequences.

**Security:** AI governance frameworks must prioritize safeguarding data and systems from breaches and misuse. Employing strong encryption, regular security audits and maintaining a robust data governance strategy are essential to protecting sensitive and proprietary information.

## Why AI governance matters

As the AI revolution intensifies, strong governance becomes a key business ally. “If you don’t have a well-defined framework or clearly articulated responsibilities, things are going to slip through the cracks, and that can have significant unintended consequences on individuals and groups. Data breaches, for example, can carry steep fines that are enough to shut companies down,” explains Sucharita Venkatesh, senior director, risk management, at Publicis Sapient.

In other words, a robust governance framework helps with AI risk management while also ensuring companies keep pace with new, emerging regulations.

## Business and compliance risks

The business world will have to navigate a maze of AI regulations—and eventually ones that haven’t even been written yet. Compliance isn’t about avoiding fines; it’s about building solid trust from the get-go. Take the [General Data Protection Regulation](#) (GDPR) in the European Union, for instance, which promotes data governance. It sets stringent rules for how companies should handle and protect data.

For organizations that provide consumer services, AI compliance means securing and protecting data, which in turn helps maintain customer trust and the brand’s reputation. For example, a European retailer using AI for personalized marketing must track and manage customer consent for data usage diligently, making sure they align with GDPR and other local laws.

Meanwhile, regulations like the [EU AI Act](#) provide comprehensive governance frameworks that influence how companies develop and deploy AI technologies.

“It’s going to have wide application because it’s not just applicable to products and technologies made in the EU. Anything you’re releasing in the EU is fair game,” Venkatesh says. “The AI Act has different levels of risk associated with different kinds of systems. And then there’s certain kinds of unacceptable risks, which are directly prohibited. You can’t use AI for social scoring. Anything that carries a high or system risk needs to be registered with the central authority and needs to be monitored. Companies will also have to publish details about how they’ve tested and put plans in place to mitigate the risk.”



All it takes is one incident for your company to completely lose its credibility. It doesn’t matter if you had 100 successful projects. One bad incident is going to hit you.

**Sucharita Venkatesh**

Senior Director, Risk Management, Publicis Sapient

## AI ethics and trust

Any new technology brings the risk for harms, both known and unknown. And the best way to manage risks? According to Venkatesh, “Make sure you have ethics and governance structures in place that allow you to think through the harms that can come with AI and the mitigation strategies you need.”

AI ethics covers a broad scope of issues, from making fair decisions to making sure that actions don’t lead to inequalities.

Why is this important? When organizations [build ethical AI systems](#), they signal to their customers that they are committed to enacting their values and delivering products or

services that benefit their customers. Trust hinges on ethical and responsible AI.

“As an example, you may use automation to help you with loans,” she says. “If there is bias in the system, then you’re cutting off a whole group of people who could have access to these loans but are being denied them due to these biases.”

The risk of bias isn’t limited to the financial services industry. According to 2025 research published in *Nature Medicine*, large language models have biases baked into them that [give medical diagnoses based on sociodemographic labels](#), which means that the systems don’t treat patients equally and could potentially put their health in jeopardy.

How can you avoid these risks and build trustworthy AI systems and processes? With the help of a governance framework.

## Key components of an AI governance framework

AI governance can seem intimidating at first, especially if you’re focusing on what you don’t know. According to [2023 Gartner research](#), for example, IT and data analytics leaders cited issues like skill gaps (57 percent), a lack of understanding about the effect that AI has on their business (38 percent) and stymied collaboration (22 percent) as key challenges that they faced while building out their governance framework.

A solid AI governance framework doesn’t just magically appear overnight. Instead, you need to build it, brick by brick, in a way that works for you.

“It doesn’t have to be a bottleneck,” says Renaud Baguena, group vice president, global head of risk management at Publicis Sapient. “You can make it very flexible, very fast. When companies fail is when you’re either underthinking or overthinking it. At the end of the day, governance just means appointing a set of people who are accountable for defining a strategy, making decisions and ensuring every activity is executed according to such decisions.”

The right kind of governance framework will address key elements that align AI systems with ethical guidelines and your organization’s goals.

And you don’t necessarily have to start from the ground up. “Building a governance framework doesn’t necessarily require you to invent things from zero,” says Todd Cherkasky,

group vice president, customer experience and innovation consulting. “You’ve got lawyers in place that are looking at policies that are already anticipating some regulatory changes, for example, so you could do an assessment about where the gaps are. The goal is to supplement existing policies and frameworks and make them more durable.”

## Organizational structure and roles

Want to get governance right? Start with identifying clear roles and responsibilities. This could mean appointing a CAIO or leveraging current leaders to take charge of AI oversight. Their job is to bring different departments and teams together to seamlessly put policies into practice.

“You should make sure your governance team is cross-functional,” Baguena explains. “You need data people. You need engineering people. You need lawyers. You need sales people. Make sure that all those people are in a room and empowered to have conversations, to have disagreements. And you should also have someone who is a kind of referee, who serves as the whistle in the game and makes decisions because it’s their job.”

He adds, “You need to empower the experts in their own domain to do the right research because they have 10 years of study in their domain. For example, an employment lawyer needs to tell you what the impact of AI is in employment regulation. Same for data privacy. Get the expertise where it is; you need experts to weigh in, then the company can make a decision.”

At the same time, governance isn’t in the hands of a select group of people. “Governance is everyone’s responsibility. It’s not just accomplished by having a team or working group set up with a name,” emphasizes Cherkasky. To ensure that everyone is aligned on governance, organizations should invest in “[awareness, learning and development, empowering and resourcing](#).”

Global organizations have the added challenge of designing governance frameworks that need to be flexible enough to meet different regulations in different regions. They might establish localized AI governance roles to ensure compliance with regional variations in data protection laws and cultural expectations so that global strategies meet local needs.

## Policies and procedures

Strong policies and procedures are the backbone of any AI governance framework. Governance committees craft these to set ethical boundaries and define what's permissible for AI technologies within their organization. Legal teams, AI experts and ethical committees typically work hand-in-hand to develop these policies.

Procedures should lay out guidelines for ethical use data, timelines for regular audits and plans for continuous improvement. Compliance frameworks help organizations stay on track with both current and new legal requirements.

## Risk management and monitoring

Effective AI governance thrives on robust risk management strategies. It's not just about reacting to issues but also proactively identifying and mitigating potential problems. Regular audits and real-time monitoring can flag anomalies and assess performance.

"Make sure you know where your data is coming from and that you're auditing your algorithms regularly," says Venkatesh. "Get a third-party audit and document everything thoroughly." Leveraging advanced monitoring tools, businesses can track AI models in real time, identifying deviations from expected outcomes and facilitating rapid corrective measures.

*[Ready to de-risk your generative AI implementation? Check out our AI risk management playbook and learn how to overcome common challenges.](#)*

## AI governance tools and technology

Auditing, compliance reporting and strategic planning—these all need the right tools. Interest in AI governance software is only accelerating, with [Forrester projecting that businesses will spend \\$15.8 billion on it by 2030](#) [↗](#).

With features like model monitoring dashboards, bias detection algorithms and real-time reporting tools, AI governance platforms make oversight easier by enabling performance tracking to that you can be sure you're adhering to regulatory standards.

Visual analytics tools also help organizations make sense of processes and outcomes, which helps stakeholders get a 360-degree view of how AI works. Finally, you can layer in tools

and techniques like differential privacy to protect individual data.

You don't need to implement all the tools at once. "There are different tools and strategies available at different stages," says Venkatesh. "Use the right solutions that you need."

## Best practices for implementing AI governance

What does successful implementation look like? Organizations need to define strategies and best practices. Here's how you can get it right:

**Align AI governance with your business strategy:** Making sure AI governance seamlessly [fits into your business strategy](#) will keep everything moving in the right direction, aligned with goals and needs. This means weaving AI governance into strategic plans and showing how it will contribute to overall success.

Collaborative workshops with leaders from different business units can identify common goals and address concerns related to AI deployment. This sees to it that governance efforts will meet everyone's objectives.

And don't overlook your company's north star in this process. "A company's core values can be used to help inform the organization's principles and the behaviors that employees are expected to enact—and that's all part of governance," points out Cherkasky.

**Establish governance boards and ethics committees:** Governance boards and ethics committees are instrumental in overseeing AI initiatives. They should include a mix of folks from IT, legal, HR and external ethics experts to give a well-rounded view on implementations. Their job is to review AI projects, offer strategic guidance and make sure all AI systems follow ethical standards. For multi-national companies, setting up localized committees helps address local nuances more effectively.

**Monitor AI models continuously:** Want to catch any performance hiccups and keep governance on track? You'll need to regularly monitor your AI models. AI lifecycle management tools can automate tracking so that your models get frequent updates and performance evaluations. This continuous monitoring should go hand-in-hand with policy reviews to keep them relevant as technology and regulations change. Setting up feedback loops with end users can also identify opportunities for fine-tuning.



## **Where AI governance is headed**

The future of AI governance is both exciting and challenging, shaped by evolving regulations and technological advancements.

### **The rise of AI regulations**

AI regulations are gaining momentum globally, with the EU AI Act representing a landmark initiative aiming to create a uniform regulatory system across Europe. Businesses need to stay ahead of the curve by proactively aligning with these evolving rules to minimize compliance risks.

Companies working across different countries and regions will have the added challenge of juggling diverse regulations while keeping practices consistent globally and flexible locally. Scalable governance models can help by addressing local legal details and expectations.

### **The role of AI in self-governance**

AI itself can be a game-changer in governance. By using AI-driven tools, you can tap into the power of AI for tasks like compliance monitoring, identifying risks and harvesting predictive insights. These tools can audit processes on their own, flagging potential issues and confirming that models and processes are honoring the policies.

Imagine having AI software that detects anomalies in financial transactions and report irregularities automatically, freeing up finance teams to focus on strategic priorities. By boosting human decision-making, AI makes governance more precise.

### **The future of AI governance starts now**

When companies build strong governance into their AI strategies, they're better equipped to navigate the complexities of AI deployment. This approach not only encourages responsible innovation but also lays a foundation of trust and integrity. Prioritizing AI governance sets

organizations apart in a competitive market, showcasing their commitment to fairness, security and transparency in how they use technology..

As AI continues to evolve, businesses must remain agile, adjusting their governance strategies to anticipate regulatory shifts and taking advantage of AI's capabilities to refine processes. By doing so, they'll not only manage risk but also open new doors to growth and innovation.

## Related Topics

---

[AI Ethics](#) | [Data Governance](#)