TrendAI™ Research

# Why Unmanaged AI Reliance Creates Business Risk

Large language models (LLMs) are rapidly being integrated into critical business processes, including customer-facing products and public communications. While AI integration is a key driver of near-future innovation, our research shows how its rapid deployment, combined with unmanaged reliance on AI models, can lead to material business risk.

As AI becomes more deeply involved in business and government operations, missteps are more likely to translate into financial loss, reputational damage, and exposure, particularly when AI outputs are not adequately verified or governed.

# Key Findings

Our team ran thousands of repeated experiments against almost 100 models, using a set of over 800 provocative questions covering regional biases, geofencing, data sovereignty, censorship and more. This allowed us to probe AI model responses to uncover the risks most relevant to businesses today.

This research aims to equip organizations with a more informed outlook on how to leverage this decade defining technology.

## Unverified AI Responses Create Direct Business Risk

Organizations that blindly rely on LLM outputs, especially in business processes with customer-facing outputs, expose themselves to the risks of AI bias that can result in:

- Legal and regulatory consequences
- Financial penalties
- Customer churn and loss of trust

## Bias is Inherent and Contextual in AI Models

AI outputs differed significantly based on the user's region and geolocation, particularly on politically sensitive topics such as national identity and territorial disputes. AI models we observed exhibited varying degrees of:

- Political and geopolitical bias
- Societal, cultural, and linguistic bias
- Computational bias

## Unmanaged AI Model Outputs Can Implicitly Define Organizational Stance

Even simple features that rely on AI can have unintended consequences. In one example, models differed significantly in how they represented a country's identity, effectively embedding geopolitical positions into AI outputs.

## Non-Deterministic Nature of AI Undermines Predictability

Unlike traditional software systems, LLMs do not consistently produce the same outputs for the same inputs. This variability complicates:

- Governance and auditability
- Risk assessment
- Regulatory compliance

## Regional Controls Limit Access and Influence Output

Different factors introduce inconsistency in global deployments and uneven user experiences. The research identified:

- Censorship of sensitive topics in certain regions
- Data sovereignty signals influencing responses
- Geofencing that restricts access or alters outputs based on user location

# What Organizations Can Do To Mitigate Risk From AI Bias

Awareness of these risks is the most powerful defense any organization has as it adapts to AI, a decade defining technology. The strategies presented here provide a starting point.

**Establish a governance framework**

Designate clear executive ownership of AI deployment, require human oversight for user-facing AI outputs, and ensure transparency from third-party AI vendors on models, data sources, and embedded controls

**Audit and monitor AI systems**

Validate training data and use cases before deployment, test regularly as models change regularly, continuously monitor AI behavior to detect risks early, and prioritize explainable AI where possible

**Build a risk-aware culture**

Define the organization's stance on sensitive topics, invest in diverse teams, conduct AI ethics training, and empower employees to question and escalate AI-related concerns