Deloitte. | databricks

FALL 2025

Navigating AI & Data Risk for Insurers: *Perspectives on AI Governance, Fairness & Trust*

TO DELICATELY BALANCE INNOVATION, STRATEGY, & RISK, *BOTH INSURERS AND REGULATORS ARE ASKING THREE FUNDAMENTAL QUESTIONS …*

1

HOW CAN INSURERS ENSURE AI DECISIONS ARE FAIR & TRANSPARENT?

What governance and oversight mechanisms are needed so that AI-driven outcomes are explainable? What governance, transparency, and accountability measures ensure AI-driven decisions are fair and in the best interest of policyholders?

2

ARE TODAY'S RULES READY FOR TOMORROW'S RISKS?

Do existing laws and regulations adequately address the unique risks of AI—such as bias, discrimination, and lack of explainability—or will a new regulatory framework come forward to keep pace with innovation?

3

IS THE DATA GOOD ENOUGH—AND SAFE ENOUGH—FOR AI?

How is the data fueling AI models assessed for accuracy, security, and compliance? How do insurers manage and oversee not only their own AI systems but also those provided by third-party vendors?

Deloitte and Databricks have a shared focus on AI and Data risk management, helping insurers to deploy secure and trusted AI solutions. In this report, we explore these questions to help organizations maximize business value while driving a competitive edge with governance, fairness and trust.

How can insurers ensure AI decisions are fair & transparent?

Robust governance, transparency, and accountability are essential for ensuring AI-driven decisions are fair, explainable, and in the best interest of insurers & consumers

GOVERNANCE

Board and Executive Oversight:
Clear responsibility for AI risk at the highest levels

Enterprise Risk + AI & Data:
Elevated identification & monitoring for data and AI risks, aligned to broader enterprise risk management framework & strategies

TRANSPARENCY

Model Risk Management & Reporting:
Robust, ongoing processes to identify, assess, monitor, and mitigate risks throughout the AI model lifecycle, and decision logic to support audits and regulatory reviews

Third-Party Data Oversight:
Contractual and technical controls to ensure third-party vendors use insurer data only for agreed purposes, with rights to audit and monitor data practices.

ACCOUNTABILITY

Independent Audits:
Regular, independent audits of AI models for bias, fairness, and regulatory compliance

Recalibration across all 3LOD:
Refreshed definition of accountability & enhanced monitoring techniques to address areas of evolving AI & data risk

Additional references: Databricks Data AI Security Framework; Deloitte Trustworthy AI Services; Deloitte Data Risk Management

Are today's rules enough for tomorrow's risks?

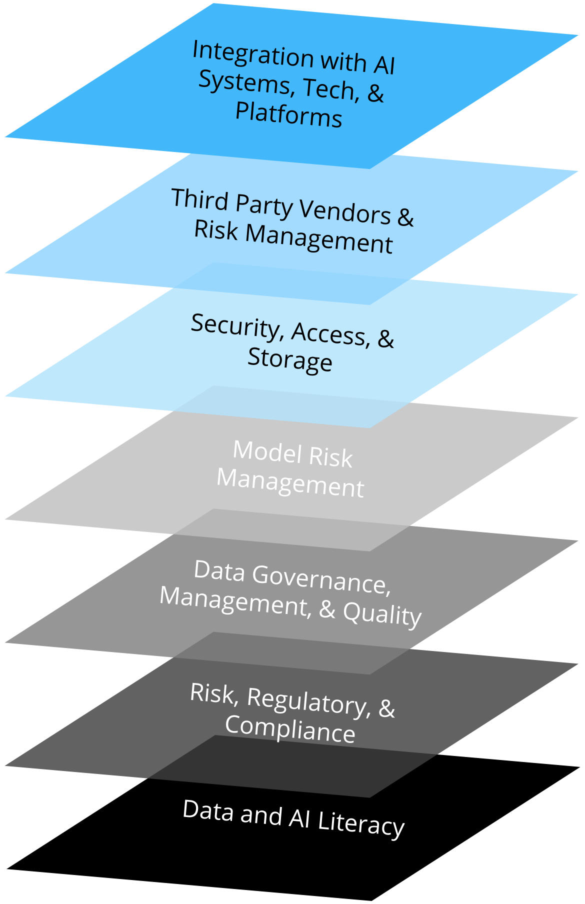
Today's regulatory and legal frameworks provide a robust foundation for both insurers and consumer protection priorities, but a variety of emerging risks are unique to the use of AI models and solutions – ***for both insurers and consumers.***

		EVOLVING IMPLICATIONS FOR THE USE OF AI	
Example Risks (Non-exhaustive)		***For Insurers***	***For Consumers***
Reputation & Consumer Trust	Misuse of AI (perceived or real) erodes trust and reputation	Loss of business, brand damage	Reluctance to engage, reduced satisfaction; industry perception
Algorithmic Bias	AI models may produce unfair or discriminatory outcomes	Regulatory penalties, reputational damage, legal challenges	Unfair denial of coverage, higher premiums, discrimination
Lack of Explainability	AI decisions are difficult to interpret or justify	Difficulty in regulatory compliance, loss of stakeholder trust	Lack of transparency, inability to challenge decisions
Model Errors & Drift	AI models may degrade or make errors over time	Financial losses, incorrect pricing/underwriting, compliance risk	Unjustified claim denials, inaccurate policy terms
Data Privacy & Security	Large data requirements increase exposure to breaches and misuse	Regulatory fines, loss of customer trust, operational disruption	Exposure of personal data, identity theft, privacy loss
Data Quality & Bias	Poor or biased data can lead to flawed AI outcomes	Faulty risk assessments, regulatory scrutiny	Inaccurate risk profiles, unfair treatment
Cybersecurity Vulnerabilities	AI systems may be targeted by cyberattacks	System downtime, data loss, ransom demands, regulatory scrutiny	Service disruption, data compromise, financial loss
Accountability & Liability	Unclear responsibility for AI-driven decisions	Legal uncertainty, increased litigation risk	Difficulty seeking redress for errors or harm
Systemic Risk	Widespread adoption of similar AI models can amplify industry-wide failures	Market instability, correlated losses, regulatory intervention	Reduced industry reliability, potential for mass impact

Additional references: Databricks Data AI Security Framework; Deloitte Trustworthy AI Services; Deloitte Data Risk Management

Is the data good enough —and safe enough— for AI?

Insurers should take a broad, layered approach to ensuring that their data is both "good enough" (high-quality, reliable, fit-for-purpose) and "safe enough" (secure, compliant, and ethically managed) for AI-driven models, solutions, and operations


Integration with AI Systems, Tech, & Platforms
Third Party Vendors & Risk Management
Security, Access, & Storage
Model Risk Management
Data Governance, Management, & Quality
Risk, Regulatory, & Compliance
Data and AI Literacy

PRIORITY FOCUS AREAS	
Tech & Data Integration	• Platform compatibility, scalability • Seamless data pipelines • Automated monitoring • Next-gen catalog & accessibility
Third-party	• Vendor data processes & security • Contractual safeguards for breach & protection • Oversight for data quality & security
Security	• Access controls and least-privilege • Encryption, tokenization, masking • Incident response
Models	• Bias and fairness audits • Model monitoring & drift • Input data validation and inference
Data	• Policies & procedures; accountability • Data accuracy, completeness, timeliness, consistency • Standardization, validation, cleansing
Risk, Regulatory, & Compliance	• Evolving legislative priorities (US, global) for data, privacy, security, and AI • Evolving measures for compliance, reporting, and monitoring
Data & AI Literacy	• Training programs • Data ethics and bias • Culture of accountability and proactive risk management

Additional references: Databricks Data AI Security Framework; Deloitte Trustworthy AI Services; Deloitte Data Risk Management

The case for Databricks

Databricks provides a unified platform for managing large, diverse datasets—essential for insurers who rely on complex, high-volume information from claims, underwriting, customer interactions, and external sources. This foundation enables accurate, reliable AI models and reduces risk by ensuring data quality and governance.

Deloitte delivers a Trustworthy AI$^{\text{TM}}$ framework that assists insurers to identify, mitigate and manage AI risk. **This trusted framework can be integrated with the Databricks Data Intelligence Platform** to help organizations securely embrace the benefits of AI and enable innovative solutions that address the most pressing data challenges.

This collaboration can help insurers balance innovation with trust, accelerating adoption while managing risks related to AI bias, safety, and societal impact.

Trustworthy AI with Databricks

Leveraging the Databricks Data Intelligence Platform to address AI regulatory requirements with:

AI SAFETY & SECURITY | **PRIVACY** | **TRUST & FAIRNESS**

REGULATORY CHARACTERISTICS		TRANSLATED RISK		DATABRICKS DATA INTELLIGENCE PLATFORM
Model Sharing Requirements	→	*Noncompliant Model Selection, Model Locked, No Model Weights Access, Model Assets Leak*	→	*Databricks Marketplace, Unity Catalog, MosaicML*
AI Safety	→	*Query Audit, Access Policies, Input/Output Theft*	→	*External Models*
Reliability	→	*Source Data Poisoning, Raw Data Poisoning*	→	*DLT, Delta Sharing, Clean Rooms, Delta Lake*
Privacy-Preserving Techniques, Data Governance	→	*Privacy Preservation, PII Masking, Lineage Audit*	→	*Unity Catalog*
Transparency, Trustworthiness	→	*Model Drift, Model Bias*	→	*MLFlow, Lakehouse Monitoring*
Data Safety	→	*Data Confidentiality*	→	*Unity Catalog, Clean Rooms, Model Serving*
Managing Bias, Explainability	→	*Data Accuracy, Bias*	→	*Model Monitoring, Unity Catalog*
Fairness, Responsible AI	→	*Bias, Protected Classes*	→	*Lakehouse Monitoring, OSS AI Tooling on Databricks Platform*

What's next?

Secure AI and data risk management enables insurers to launch new products, enhance claims processing, and personalize customer experiences—all while maintaining the regulatory and reputational standards essential for long-term growth.

Leveraging Databricks for trustworthy AI enables insurers to innovate securely and responsibly, driving both growth and confidence in their market offerings.

Deloitte. | databricks

Connect with us

Cory Liepold
Principal
Deloitte & Touche LLP
cliepold@deloitte.com

Courtney Parry
Principal
Deloitte & Touche LLP
cparry@deloitte.com

Satish Iyengar
Managing Director
Deloitte & Touche LLP
siyengar@deloitte.com

Ajay Ravikumar
Senior Manager
Deloitte & Touche LLP
ajr@deloitte.com

Nick Mozena
Senior Manager
Deloitte & Touche LLP
nmozena@deloitte.com

David Zalk
Manager
Deloitte & Touche LLP
dzalk@deloitte.com

Sathish Marimuthu
Managing Director, AI & Data
Deloitte Consulting LLP
satmarimuthu@deloitte.com

Shiva Govindaraju
VP Sales Executive, Databricks Alliance
Deloitte Consulting LLP
shgovindaraju@deloitte.com

Omar Khawaja
CISO
Databricks
omar.khawaja@databricks.com

Anindita Mahapatra
Principal Solutions Architect
Databricks
anindita.mahapatra@databricks.com

Erin Butler
VP, Financial Services Sales
Databricks
erin.butler@databricks.com

Kim Hatton
Financial Services Marketing Leader
Databricks
kim.hatton@databricks.com

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Product names mentioned in this presentation are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.