E-ISSN : 2455-5703
GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Synthetic Intelligence and Predictive Risk Modeling in Digital Insurance Platforms

Bhasker Katta
Independent Researcher
kattaabhasker@gmail.com

Abstract

Generative AI-driven next-generation risk-intelligence platforms enable insurers to replicate human-intuitive reasoning, generate new risk signals, and optimize decisions across the risk and compliance processes with minimal human intervention. Recent technological advances in generative modeling and foundation models make this now possible, and could herald a renaissance in insurance. However, AI tools for risk data and decisioning remain in their infancy. Consequently, an understanding of how generative techniques can fuel the architecture, taxonomies, and use cases of risk-intelligence platforms is essential to making the insurance future safer for all. The research proposes a comprehensive exploration of these dimensions by answering three questions: How can insurance decisioning in risk and compliance processes be transformed into a generative problem? What foundational risk taxonomies and use cases underwrite next-gen AI platforms for underwriting, pricing, fraud detection, and prevention? What criteria can evaluate, scrutinize, and bolster these models?

The findings propose a structured framework for harnessing generative AI in risk intelligence and empowering a new generation of predictive tools for insurers. Focusing on the underlying concepts and considerations simplifies comprehension, encourages organizational readiness, and highlights a roadmap for best practices—key for the secure deployment of robust generative-driven solutions as market demand burgeons.

Keywords : Generative AI in Insurance,AI Risk Modeling,Predictive Risk Analytics,Intelligent Underwriting,Automated Claims Processing,Fraud Detection AI,Dynamic Risk Assessment,InsurTech Innovation,Machine Learning Risk Scoring,Real-Time Data Analytics,AI-Powered Actuarial Models,Personalized Insurance Pricing,Natural Language Processing (NLP) in Insurance,Risk Intelligence Platforms,Next-Gen Insurance Technology.

1. Introduction

By any measure, the world has entered an era of unprecedented uncertainty. Risks from pandemics, climate change, war, economic crises, and cyber threats are becoming more pronounced and visible, while new high-impact and low-probability risks—such as systemic risks to artificial intelligence and social networks—are emerging. Technologies deployed to process an expansive volume of structured and unstructured data related to the physical world have transformed consumer markets in almost every domain. Yet the paradigm shift in the insurance sector—one that should come from an AI-first, real-time, outside-in risk-ecosystem platform approach—has been sluggish, muddled, and inadequate.

These considerations justify a rethink of the data-driven-model phenomenon and its application to risk areas beyond underwriting—such as pricing, fraud detection, case management, and the broader WRAP market (weather, renewable assets, agribusiness, pandemic)—for which risk and pricing signals remain too patchy and error-prone. Nevertheless, a comprehensive definition of generative modeling—and how it relates to AI-driven decision-making—has yet to be formulated in the industry.

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

The following subsector reviews several crucial aspects of the enabling data ecosystem for generative-model-based risk-intelligence solutions.

1.1. Background and Significance

The global nature of the insurance business exposes insurers to a wide range of risks. Ability to rapidly analyze and characterise these risks influences an insurer's performance, management choices and strategy. Yet risk intelligence remains a gap in current generation insurance platforms. Generative AI can address this gap by ingesting past claims data as well as other internal and external signals and using these to create latent representations of risk. Automated processes then generate underlying risk factors linked to temporal dynamics and associated uncertainties, creating information to aid decisioning in areas such as underwriting, pricing, and fraud detection and prevention. A structured governance framework oversees the generation of risk signals, ensuring compliance with regulatory requirements for critical areas like fairness, bias, or privacy.

Meaningful and repeatable decisions are foundational to insurance and its risk management role in society. Expanding knowledge of risks and avoiding policyholder or stakeholder surprises is consequently key to every insurer's core market-facing activities, as well as their ongoing financial performance and market capitalisation. Specialty insurers should, therefore, constantly identify, analyze, and model emerging risks that can materially impact their business, consumers, and society at large. Generating accurate and timely insights to support these efforts requires an enterprise-wide approach to risk identification—a goal often not met in practice.

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Fig 1: Generative AI in next-gen insurance

1.2. Research design

The objectives are to define a generative AI architecture for building risk intelligence systems in the insurance domain, establish principles for risk signal design and data ecosystem formulation, and develop a use-case taxonomy with supporting evaluation and compliance considerations. It is hypothesized that risk signals constructed to meet defined criteria, modeled under the generative paradigm, and evaluated across relevant dimensions will lead to greater performance in decisioning tasks than those grounded in the discriminative framework.

Risk signals from published datasets and private sources serve to identify generative AI opportunities in insurance, and domains such as underwriting, pricing, fraud detection, and reserve estimation provide specific use cases. The proposed architecture follows a platform-based approach, guided by the principle of privacy-by-design and aligned with data engineering best practices. Complementary perspectives on model governance, use-case evaluation, and compliance considerations facilitate realization of risk intelligence systems that meet enterprise standards and regulatory mandates.

E-ISSN : 2455-5703
GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Equation 1: Joint generative risk model

Step-by-step derivation

Start from the chain rule of probability:

$$p(X,Y,Z) = p(Z)\, p(X,Y \mid Z)$$

Now expand the second term again using the chain rule:

$$p(X,Y \mid Z) = p(X \mid Z)\, p(Y \mid X,Z)$$

Substitute back:

$$p(X,Y,Z) = p(Z)\, p(X \mid Z)\, p(Y \mid X,Z)$$

Introduce model parameters θ:

$$p_\theta(X,Y,Z) = p_\theta(Z)\, p_\theta(X \mid Z)\, p_\theta(Y \mid X,Z)$$

2. Foundations of Generative AI in Risk Intelligence

Contemporary insurance platforms adopt a data-driven approach to risk assessment, which is frequently underpinned by machine-learning models. One specific aspect of such systems revolve around employing Generative AI techniques to support risk identification, quantification and management. Generative Modeling and Risk Signals in this regard refer to deriving predictors of risk from Claims Data, Exposure Data, Sensor Data and other data sources in a Data Ecosystem.

Data-driven insurance platforms rely on the successful capture, preparation and alignment of data pipelines to a Decision Chain. It is now equally important to quantify uncertainty in the predictor or signal produced and to have a storage sub-system that supports Data Sovereignty, Localization, Security, Privacy and Regulatory Requirements. Consequently, framework definition for Calibration and Validation, Robustness, Fairness and Bias-Mitigating Testing, Continuous Monitoring and Auditing, and Privacy and Security Considerations are important to operationalise Data-driven platforms. The AI Risk Signals produced are also used by Human experts to benefit from Human-Centric Intelligent Augmentation rather than attempting to Automate Legion Services.

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Fig 2: Generative AI in risk intelligence

2.1. Concepts of Generative Models and Risk Signals

Generative modeling refers to an unsupervised approach that learns the joint distribution of inputs based on available data samples and their underlying latent factors. The learned representation enables the generation of rarely or unseen combinations of the supplied input variables. Risk signals expected to be generated can be viewed as a representation of the joint distribution of risk and its latent factors. The level of risk is influenced by a combination of external conditions and internal factors of the insured entity, which change over time. The corresponding representation becomes essential for loss estimation, allowing the assessment of conditions or scenarios with little or no historical preceding, calibration of premiums, scoring of risks, validation of model outputs, segmentation of exposures, and maintenance of future scenarios with regard to rare external events.

Because insurance involves uncertainty over a time horizon, the evolution of the risk joint distribution, along with its uncertainty quantification, becomes a critical requirement for decision-making processes during underwriting, pricing, reserving, and risk transfer. The distribution incorporates latent relationships between the insured and the risk transfer entity that become evident only in hindsight, leading to detection of anomalies and fraudulent acts. A well-designed management pipeline can signal risks for various insurance functions, including underwriting and pricing, fraud detection and prevention, and handling of claims and recoveries.

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

2.2. Data Ecosystems for Insurance Risk

Data ecosystems for insurance behavior embrace the data sources, types, quality aspects, and data governance needed for generative AI models used within an insurance organization. The risk intelligence ecosystem leverages the full spectrum of data that influences insurance risk, with a dual focus on emerging behavior in claims data and exploration of factors by risk category through other sources.

Data types can be categorized into four key buckets: claims and other loss information, exposure data, sensor data, and external feeds (e.g. weather, geolocation, economic indicators) The first two are generally owned by the organization, while the external data is consumed as special-purpose data pipelines or APIs. The more complex and important sensor data requires a clear strategy with respect to quality, integration, and governance.

Data quality dimensions for all categories span completeness, correctness, accuracy, consistency, uniqueness, and timeliness. Quality across the first three is largely determined by the health of the source system, while uniqueness is addressed through integration. Timeliness, which has implications not only for system design but also for visualizations at business-unit and executive levels, can be challenging for unstructured/natural-language sources.

Equation 2: Posterior risk signal

Step-by-step derivation

From Bayes' rule:

$$p(Z \mid X) = \frac{p(X \mid Z)p(Z)}{p(X)}$$

where

$$p(X) = \int p(X \mid Z)p(Z)\, dZ$$

if $Z$is continuous, or

$$p(X) = \sum_{Z} p(X \mid Z)p(Z)$$

if $Z$is discrete.

So:

$$p_\theta(Z \mid X) = \frac{p_\theta(X \mid Z)p_\theta(Z)}{\int p_\theta(X \mid Z)p_\theta(Z)\, dZ}$$

Now define a risk signal as the posterior expectation of a latent risk function $g(Z)$:

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

$$R(X) = \int g(Z)\, p_\theta(Z \mid X)\, dZ$$

3. Architectural Considerations for AI-Driven Platforms

A multi-stakeholder approach is needed to drive innovation in data-driven risk sensing. The emergence of generative AI models signals new opportunities for next-generation insurance platforms. These platforms can enable insurance companies to harness generative AI techniques to transform proprietary and public data into risk signals that assist underwriting and pricing, loss prevention, fraud detection, and more.

The design phase encompasses a range of considerations crucial to the successful development and deployment of generative risk signals. Data ingestion and integration pipelines are responsible for acquiring the large volumes of internal and external data required to train generative models. Robust governance frameworks ensure that the models comply with institutional policies and regulatory requirements throughout the entire modeling lifecycle—from development through deployment, maintenance, and retirement.

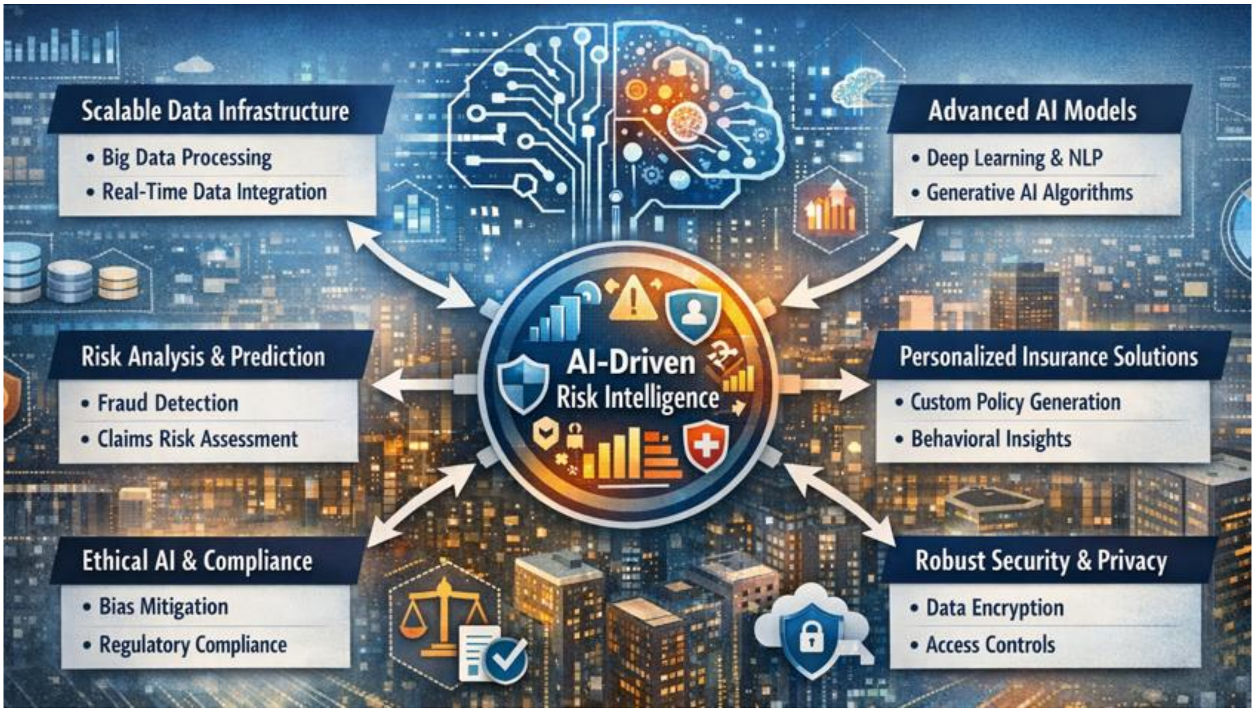


Fig 3: AI-driven insurance platform architecture blueprint

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

3.1. Data Ingestion and Integration

Scalable ingestion pipelines are vital for high-throughput production AI systems. Theft and Life & Health Insurance are presenting additional operational loss potentials, creating new use-case opportunities for Fraud Detection and Prevention. Growing amounts of data from IoT sensor devices and 3rd-party geolocation feeds have the potential to further augment claims. Therefore, integrated multi-dimensional risk scoring for all insurance segments is both strategically relevant and imperative. This includes the identification of new underwriting insurance opportunities or even outside traditional business domains.

Real-time incrementality is paramount to keep the risk insights and alerting capabilities fresh. Data sources across the spectrum of Life & Health and Non-Life Insurance Fraud indicators must, therefore, be consolidated into a layered Real-time Data Ingestion architecture providing low-latency capability. Such an architecture forms the foundation for ingestion pipelines that allow high-throughput computational demand for detection within Data Taxonomies and Scoring Models. Ongoing calibration insights establish the data distribution and temporal dynamics, enhancing continual model accuracy improvement and uncertainty quantification. Data pipelines must therefore be managed as Product Pipelines for Data in Motion where Data Quality, Validation, Monitoring, and Lineage are key areas of concern and management capacity.

A data catalogue is a primary tool for effective Data Quality and Governance. It details the attributes of ingested data by business-friendly relation, describing the value and relevance from a business point of view. Data, rules, alerts, and remediation initiatives for incrementality, provenance, and lineage, among others, also undergo strategic management from the Data Catalogue. It ensures real-time data validation through metadata on quality thresholds, thresholds for time lag, and fresh data updates. Alerts for rule breaches get incorporated into a remediation backlog properly prioritized against risk implications for the business. Data Quality is strenuously monitored to ensure detection model accuracy, improve detection performance, and trigger training shifts for Scoring Models and Risk Taxonomies.

Data bucket	Typical contents	Primary insurance value	Governance notes
Claims and loss information	Claims files, case notes, historical loss outcomes	Detects patterns, anomalies, leakage, recovery opportunity	Sensitive personal data; quality tied to source-system health
Exposure data	Customer, policy, asset, location, portfolio attributes	Supports risk scoring, segmentation, premium calibration	Must remain current and uniquely integrated
Sensor / IoT data	Telematics, industrial sensors, device streams	Supports real-time detection, prevention, and dynamic risk updates	Integration quality and timeliness are critical
External feeds	Weather, geolocation, economic indicators, public data	Adds outside-in risk context and scenario analysis	API governance, provenance, localization, and refresh cadence matter

Table 1: Insurance data ecosystem

GRD JOURNALS
E-ISSN : 2455-5703
info@grdjournals.com
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

3.2. Model Governance and Compliance

A governance framework addresses the need for model oversight, with defined roles and responsibilities to guide new and changed models throughout the lifecycle. Application and cognitive domain owners approve models for production. A comprehensive register maintains model lineage, explains design choices, and documents testing and validation evidence, including calibration, reliability, and fairness results.

Independent model validation teams check models for compliance with internal standards and regulatory guidelines. Validation procedures include backtesting, holdout evaluation, and testing on out-of-time or out-of-sample data. External audits may adapt internal validation for further assurance. Regulatory requirements for transparent model governance are incorporated into operational design, documentation, and preparation for independent validation. Each model is tagged with versioning information that indicates whether the model is production-ready or requires internal or external validation. Ongoing monitoring of model performance, including key validation metrics, is essential for maintaining trust-based adoption and avoiding model failure.

4. Risk Taxonomies and Use Cases

For insurance platforms, growth relies on sound underwriting and pricing decisions and susceptibility to fraud across the risk landscape. Generative AI techniques enhance these decisions with background risk scoring and risk signals that inform decisioning in real time or near-real time.

Background risk scores, calibrated to correlate with business-relevant outcomes, support demand forecasting, optimal customer segmentation, and pricing, while providing a tool for scenario analysis through “what if” questions. Risk signals denote some relevant temporal dynamic, helping to signal the onset of a weather event or other latent risk that could result in claims, fraud, or other material business impact. Signal generation and indicator identification are prima facie tasks for generative models. Insights from generative AI also play a role in fraud detection, exploring the distribution of business-as-usual behavior to identify anomalous cases worthy of further investigation.

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Fig 4: Generative AI for insurance risk analysis

4.1. Underwriting and Pricing

Insights generated by an AI-driven risk intelligence platform can significantly enhance decision-making in underwriting and pricing applications across both personal and commercial lines of business. Risk scoring/assessment services assign risk scores at the individual customer level, while premium calibration services enable the pricing function to assign premium values based on risk characteristics. Risk segmentation identifies customer segments for which special considerations are warranted. Scenarios involving changes in customer attributes or external factors, such as the weather, can be analyzed to assess the potential impact on customer, portfolio, or channel levels. Generative models offer a layer of explainability and transparency; they help enablers understand how specific customer attributes influence the various decision-making outputs.

In a changing environment, traditional loss development methodologies may not hold, making it essential to investigate potential changes in claim cost dependencies on a range of factors. Such factors may include frequency dependence on inflation, dependence on temperature change, location, or root causes to leakage; development dependence on changes in investigations involving fraud, misrepresentation, or material non-disclosure; and recovery paths in relation to specialization and requirement of concentrated resource pools. These insights can carefully inform the calibration of certain parts of the pricing function.

Equation 3: Underwriting / pricing equation

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Step-by-step derivation

Let total loss over a policy period be

$$L = \sum_{i=1}^{N} S_i$$

where

- N= number of claims
- S_i= severity of claim i

Take conditional expectation given customer data X:

$$\mathbb{E}[L \mid X] = \mathbb{E}\left[\sum_{i=1}^{N} S_i \;\middle|\; X\right]$$

Using the conditional version of Wald's identity:

$$\mathbb{E}[L \mid X] = \mathbb{E}[N \mid X] \cdot \mathbb{E}[S \mid X]$$

assuming conditional identical severities and suitable independence structure.

Now the actuarially fair premium is the expected loss:

$$\Pi_{\text{fair}}(X) = \mathbb{E}[L \mid X]$$

Insurers then add expense/risk loading λ:

$$\Pi(X) = \Pi_{\text{fair}}(X) + \lambda \Pi_{\text{fair}}(X)$$

Factorizing:

$$\Pi(X) = (1 + \lambda)\mathbb{E}[L \mid X]$$

Substitute the frequency-severity decomposition:

$$\Pi(X) = (1 + \lambda)\, \mathbb{E}[N \mid X]\mathbb{E}[S \mid X]$$

4.2. Fraud Detection and Prevention

Fraud detection and prevention processes in insurance are integral to managing loss ratios and strengthening profitability. As the

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

financial services industry becomes more dependent on digital technologies, so do the sophistication and number of fraud incidents. Insurance companies receive millions of claims each year, and the cost of false positives is enormous.

Generative AI can therefore help by detecting anomalies in claims and other data (such as marketing or standard operating procedures) that contribute to fraud detection. Anomaly detection uses historical data to identify trends and patterns in losses, transactions, agent performance, and other processes. Any activity that deviates significantly from established norms is flagged for investigation because it has a high probability of being fraudulent. In fraud detection, these fraud indicators are consolidated under a case management system with human analysts who assess, investigate, and escalate these flagged cases. The model is meant to continuously learn from these anomalies and funnel the information back into the main training data to refine accuracy over time. The implementation of AI models ensures that the process is not only intuitive and seamless but also helps guide analysts through an increasingly complex landscape.

Fighting fraud is an ongoing battle, as new schemes emerge continually. Increasingly, fraud is being committed by organized groups that recognize the opportunities apparent in a weak business process and associated controls. Stolen identities were used as a facilitator for other forms of fraud such as claims, money laundering, and theft. As claims executives and emergency services become more aware of the typical modus operandi for various incidents, fraud insights generated via data-driven analysis enable insurance companies to adopt preemptive actions.

5. Evaluation, Validation, and Performance Metrics

Established risk processes in the insurance sector depend on appropriately validated models. For risk signals generated by generative models to be credible, evaluate the outcomes against historical observations and through interpretive stress tests. The calibration, validation, robustness, fairness, and adaptive monitoring of these risk signals comprise their evaluation. The evaluation plan details the calibration and validation techniques for risk signals — how well the model quantifies risk and aligns with risks that emerge in the future — once they are implemented into production. Ongoing robustness, fairness, and monitoring metrics safeguard against adoption risks associated with generative models.

Calibration ensures that probabilities from the risk signal are valid frequencies. Hence, calibrate the output probability for each risk classification to the ratio of the corresponding event in a holdout test set. Calibration applies to both discrete and continuous assignment probabilities. Holdout validation ensures that these probabilities remain valid out of sample. Examine calibration using graphical and numerical techniques. Backtesting with operational data provides the critical test: whether a high predicted-purchase probability clustering in time aligns with material leakage in the underlying loss exposure. Tests demonstrating the significant contribution of generative-modelling features to the probability assessment provide a strong basis for its future operational use. Non-enumerated validation applies a test set to a risk signal not explicitly trained on — supporting the validity of generalisation — particularly important with high-dimensional datasets.

E-ISSN : 2455-5703
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Fig 5: Generative AI-driven risk intelligence in insurance

5.1. Calibration and Validation Frameworks

Calibration and validation of generative AI-driven models for insurance risk intelligence assess sufficiency and accuracy of risk-related signals and decisions, covering both intended and unintended aspects. Calibration methods are appropriate for continuous variable prediction, particularly for probability estimates. Backtesting compares signal distributions across risk categories. Holdout evaluations leverage a discrete dataset partition, while out-of-sample testing requires external risk information not seen during model training.

Acceptance criteria encompass both threshold and range conditions tailored to specific signal types. For example, model outputs with discrete support guide fraud detection, ideally yielding binary observations. Inspection of detected-but-not-acted-on cases provides an additional evaluation mechanism. Models must balance utility against fairness and bias considerations, with multidimensional fairness quantification.

Stress testing identifies robustness weaknesses by investigating extreme datapoints. Adversarial evaluation leverages a separate probe model to assess generation quality, with adversarial quality measures as critical acceptance criteria. Dashboards track key signal distributions, alerting on identified thresholds. Auditing features maintain a traceable activity record for auditing purposes. The agility of generative AI model retraining should reflect temporal signal dynamics, with governance steering frequency.

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Equation 4: Fraud detection / anomaly score

Step-by-step derivation

A generative model defines the likelihood of an observed case X:

$$p_\theta(X) = \int p_\theta(X \mid Z) p_\theta(Z)\, dZ$$

If a claim pattern is normal, it should have relatively high likelihood.
If it is unusual or suspicious, it should have low likelihood.

To convert low likelihood into a positive anomaly score, use negative log-likelihood:

$$A(X) = -\log p_\theta(X)$$

Why negative log?

- high $p_\theta(X)$ ⇒low anomaly
- low $p_\theta(X)$ ⇒high anomaly

Then choose a threshold τ:

$$\mathrm{Flag}(X) = \begin{cases} 1, & A(X) > \tau \\ 0, & A(X) \leq \tau \end{cases}$$

Equivalent indicator notation:

$$\mathrm{Flag}(X) = \mathbf{1}\{A(X) > \tau\}$$

Posterior fraud probability version

If a fraud label $F \in \{0,1\}$is available, then

$$p(F = 1 \mid X) = \frac{p(X \mid F = 1)p(F = 1)}{p(X)}$$

5.2. Robustness, Fairness, and Bias Mitigation

Robustness, fairness, and bias mitigation are critical aspects of responsible AI. Sufficient stress testing against various risk scenarios is required to demonstrate stability and resilience, for example, during insured loss events. Adversarial attacks help assess potential exploits and identify model hardening measures like input filtering. Fairness and nondiscrimination testing guard against unintended outcomes stemming from societal biases. Regardless of quantifiable fairness, it is essential to include catch-all monitoring of emerging disparities, with procedures for root-cause analysis and acknowledgment of residual risk.

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Longitudinal monitoring of generated risk intelligence determines how the underlying risk progresses, elucidates input features correlated with shifts in statistical distributions, and presents opportunities for calibration refinement based on emerging signal quality issues. Disruption indicators are vital for workflows dependent on change denormalization and for assessing signal validity in near real time. Additional dashboards assist in documenting idiosyncratic model behavior during specific climatic or geopolitical scenarios.

5.3. Monitoring, Auditing, and Continuous Improvement

A comprehensive controls framework involves dashboards and alert thresholds for runtime monitoring, audit trails for compliance reviews, and governance reviews to determine retraining cadences. By surfacing deviations from expected behavior and underlying causes, such a framework helps enable a feedback loop for continuous improvement and ensures that the generated insights remain trustworthy, relevant, and effective over time. For example, dashboards can flag significant changes in historical dependencies or risk group segmentation, and changes in ranking or relative scoring of exposures can warrant further investigation. Alerts can signal degraded forecast accuracy and provide the basis for scheduled retraining.

Audit trails can maintain a record of input data for each generation; deviation of model decisions from previous assessments, especially for key risks; and trend analyses of generated insights over time. Appropriate cadences for model retraining can be determined by combining these inputs with a systematic assessment of underlying factors, such as the rate of drift in input data and external signals, the relevance of the risk group definitions, and the frequency of change in other model outputs. A defined governance review process can supplement ongoing monitoring with periodic evaluations to ensure that model performance remains aligned with expectations, thresholds for retraining are appropriately set, and any required adjustments are communicated to relevant stakeholders.

Control area	What the article expects	Evidence / artifact	When applied
Calibration	Probabilities should map to observed frequencies	Calibration curves, probability error summaries	Pre-release and after material drift
Validation	Holdout, out-of-time, and out-of-sample testing	Validation pack, benchmark results, failure analysis	Before production and after major updates
Robustness	Stress testing against extreme scenarios	Stress scenarios, adversarial probe results	Before release and periodically
Fairness & bias	Multidimensional fairness quantification and residual-risk monitoring	Protected-group metrics, root-cause notes, exceptions register	Before release and continuously
Monitoring	Dashboards should track drift, signal quality, and alert thresholds	Ops dashboard, threshold log, retraining triggers	Continuously in production
Auditability	Every output should be traceable to data, model, and filters	Lineage register, versioning, audit trail	Continuous

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Table 2: Model governance and validation checklist

6. Privacy, Security, and Regulatory Considerations

Privacy, Security, and Regulatory Considerations

With privacy erosion and consumer trust unraveling as structural issues in digital technology, businesses and regulators are confronting more difficult than ever problems in the evolving trust economy. In response, the insurance industry is updating approach to data privacy. Regulatory requirements for privacy protection, data sovereignty, and compliance are unfolding across multiple jurisdictions, and requirements are evolving. Striking a balance between compliance and business opportunity is complex due to external threats to sensitive data, the large volume of data collected and processed, the existence of different country regulations, and the precedence of compliance over strategic business decisions. Future-facing businesses are opting for a privacy-by-design roadmap and not treating compliance as a box-ticking exercise.

Privacy, security, and compliance should be designed into and not bolted on to data-generative models. Requirements from the region of operation and the geos where data-providing consumers are located need to be factored in. Variables that are triggered by the presence or absence of sensitive data shapes must also be considered. On-cloud or on-prem presence of data must be specified based on the anticipated data locality regulations. Encryption, anonymization, masking, and protection can then be implemented as steps in the data path and incorporated in the design of the tools used.

Cross-border transfers of regulated data must comply with the privacy regulations of the originating location and the region where the transfer is made. Organizations must ensure that any data processors supporting an AI model for which data sharing is agreed with the user comply with the same set of privacy regulations and practices. Access to sensitive data should be authorized based on the principle of least privilege and managed through centralized control, protecting it from user misuse or manipulation.

6.1. Data Sovereignty and Protection

Cross-border data flows, particularly when engendering critical risk intelligence, are often subject to localization requirements and data sovereignty principles that aim to protect sensitive information within national boundaries. Where such regulations exist, data at rest or during processing must be isolated within approved locations. The appropriate choice of locations is determined by the state of nature and prevailing government order or conflict. Data writes, in particular, are typically highly regulated, as data sovereignty pertains primarily to the funding side of the equilibrium.

In general, an approved data architecture incorporates adherence to data sovereignty regulations and local data protection laws. These regulations often set prescriptive rules for how data at rest and in transit must be handled. Protections usually include mechanisms for encryption, anonymization, and pseudonymization of sensitive data types.

E-ISSN : 2455-5703
GRD JOURNALS
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

Fig 6: Data sovereignty and AI risk protection

6.2. Compliance by Design

Integration of regulatory requirements into the design process enhances compliance and reduces launch risk. Incorporating compliance checks into governance accelerates implementation cycles while aligning with insurance industry standards such as FSB’s Insurance Capital Standards and the European Union’s Solvency II Directive.

The Phillips Curve is a classic economic analysis-tool that demonstrates an inverse relationship between the rate of inflation and unemployment. The Phillips Curve has altered Governments’ macro-economic policy since the New Deal, and has guided Central-Bank micro-economic policy since the advent of Central Banking. Yet it is an imperfect model used improperly. The model, when used to influence trade-offs, results in a misallocation of resources.

6.3. Auditability and Documentation

Traceability of data lifecycle and model decision paths is critical in generative AI. After a request for information or insight, all

E-ISSN : 2455-5703

GRD JOURNALS

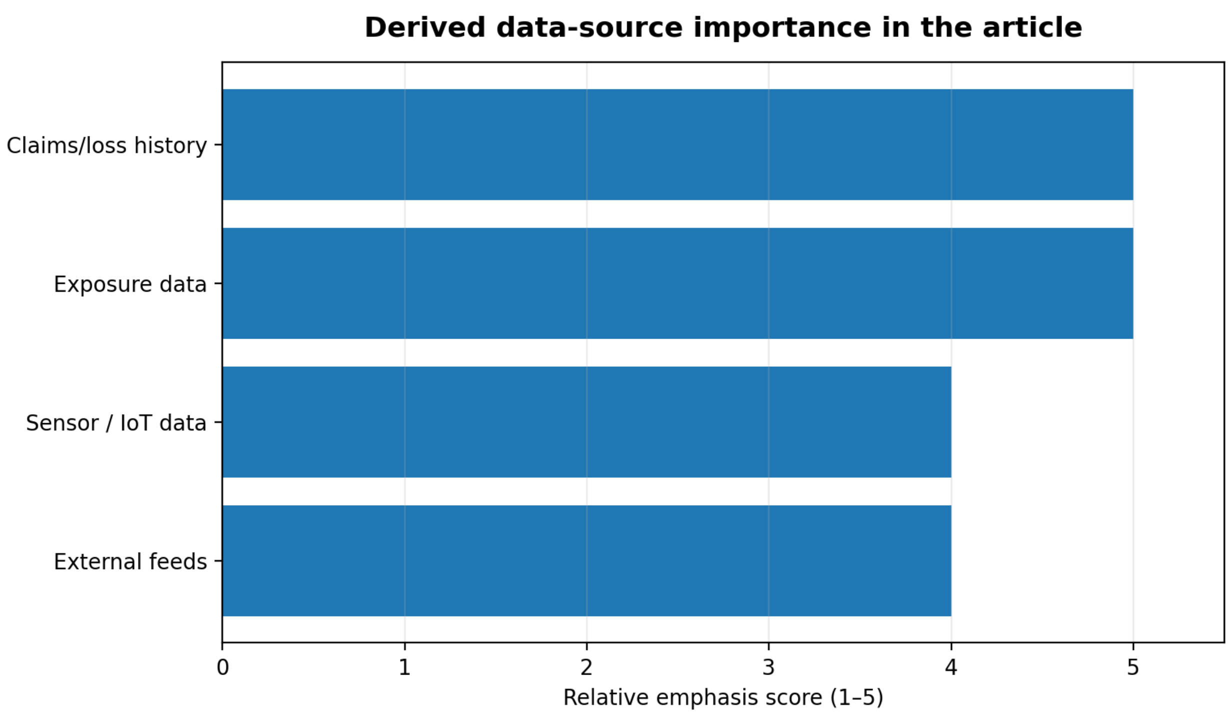
Global Research and Development Journals | grdjournals.com

Volume-04 Issue-02 JULY-SEPTEMBER 2026

info@grdjournals.com

Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

relevant elements involved in the response should be identified. This encompasses the original data sources utilized in training, the generative model generating the information, any content generation tools, the source of training data for these tools as well as the filter design, and any feedback loops. Documentation must be maintained so that the same information can be produced again for audit and regulatory purposes. This allows external oversight functions to trace the information to its original feed and consumption and verify data lineage and provenance as presented in outputs. Such auditability maintains accountability by implementing and recording oversight checkpoints when interfacing with technology. It also assists in constructing real-time dashboards for security audits and building evidence transparency toward end-consumers when the use cases relate to fairness and bias mitigation.



7. Implementation Roadmap and Best Practices

Phased approach for implementation ranging from pilot to full-scale deployment, with defined criteria for progress and exit gates, recognizing the need for iteration based on testing feedback Organizational capabilities and resources for using generative AI for risk intelligence, as well as requisite skills for the technology and business functions All elements necessary for effective exploitation of generative AI, including suitability and completeness of tools and services as well as supply-chain considerations.

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

An implementation plan guides the transition from theory to practice. The plan defines the phases of adoption, identifies controls for progress, and recognizes the need for iteration based on pilot testing. Next, it addresses organizational requirements—capability and capacity—before examining the tools and processes that support effective engagement with generative AI. The conclusions reflect these considerations and combine the earlier analysis of risk application areas with guidance from the roadmap. Supporting use cases, tools, techniques, and technologies are also included.

Equation 5: Calibration / validation objective

Step-by-step derivation

Let the model output a probability

$$\hat{p}_i = \hat{p}(X_i)$$

for observation i.

A perfectly calibrated model means:

$$\mathbb{P}(Y = 1 \mid \hat{p}(X) = q) = q$$

Example: among all policies predicted at 0.20 claim probability, about 20% should actually claim.

Since exact $q$values are sparse, partition predictions into bins $b = 1, \ldots, B$.

For bin b, define:

$$\mathrm{acc}(b) = \frac{1}{n_b} \sum_{i \in b} y_i$$
$$\mathrm{conf}(b) = \frac{1}{n_b} \sum_{i \in b} \hat{p}_i$$

Then calibration error in bin $b$is

$$\mid \mathrm{acc}(b) - \mathrm{conf}(b) \mid$$

Weight by bin size $n_b/n$and sum:

$$\mathcal{L}_{\mathrm{cal}} = \sum_{b=1}^{B} \frac{n_b}{n} \mid \mathrm{acc}(b) - \mathrm{conf}(b) \mid$$

GRD JOURNALS
E-ISSN : 2455-5703
info@grdjournals.com
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

7.1. Roadmap Phases from Pilot to Production

Translating model prototypes into production-ready solutions entails considerable additional effort. A phased validation and on-boarding plan help assess readiness at each stage and mitigate project risks, enabling incremental delivery and exploitation of early wins. The plan should define milestones, success criteria, risk characteristics, and go/no-go gates for each stage. Around these, iteration cycles can be planned for performance enhancements and capability extensions.

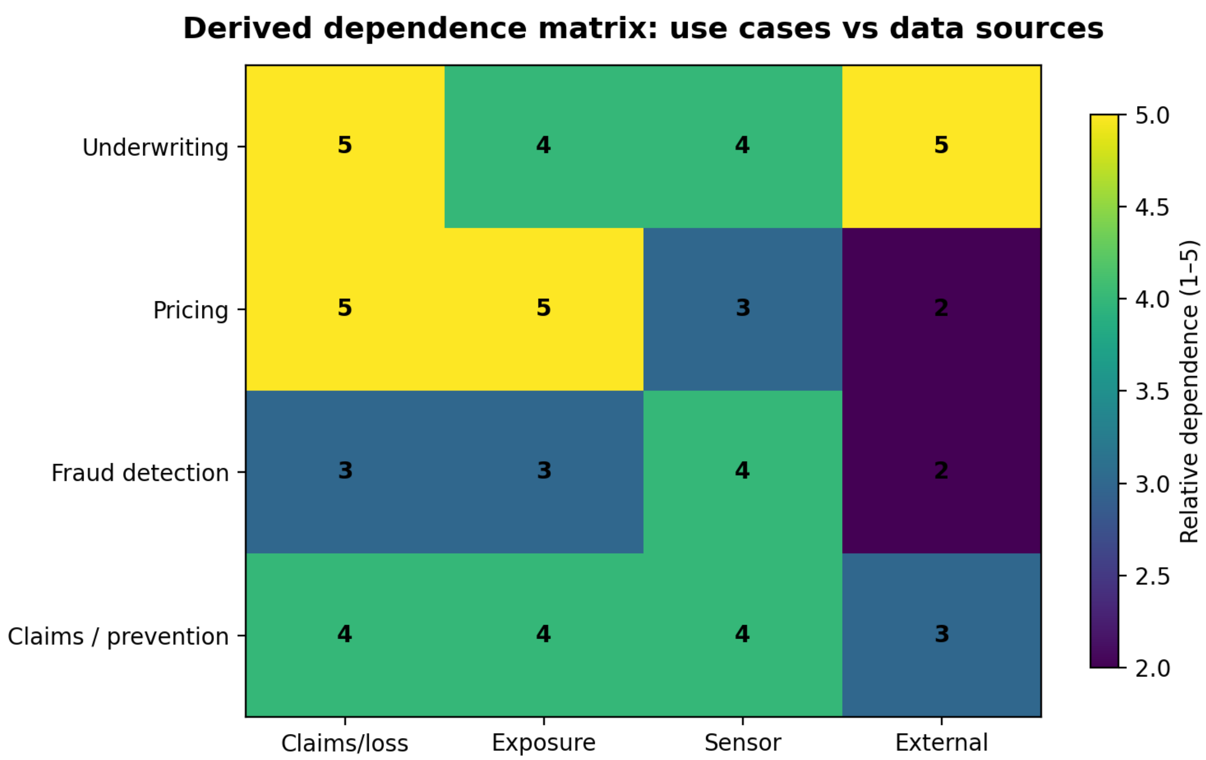
Proof of concept Pilot models are often built to test and demonstrate the feasibility of an idea without concern for robustness or scalability. Pilot models should provide evidence of business value, with success criteria aligned to deliverables or business outcomes of the function they support. Domain experts should identify potential failure modes and hidden limitations of the pilot models—such areas must be interpreted cautiously during production and used instead as triggers for deeper investigation. Pilot results should also identify the type of operational integration required for the models and the risk of such integration being exploited by criminals.

7.2. Organizational Readiness and Talent

Machine learning (ML) applications typically require competencies spanning both data science and the operational business function. When the latter function is risk-related, training the requisite talent will often involve risk professionals with domain knowledge collaborating with data scientists to prototype and train models. These groupings can subsequently evolve into production units responsible for the ongoing performance of models and data pipelines that generate and use the risk signals.

There is also a strong need for effective and trusted ML systems. The skill of running a bank, insurance company, or any other ML-dependent organization in a trusted manner is new and nascent. Such organizations will become successful not because they are beacons in the field of responsible AI; they will prosper if they can demonstrate compliance with the rules and regulations of their industry and the regions in which they operate. Consequently, the organizational readiness assessment must focus on the management of the three elements essential to risk management: ML operations (MLOps), ML governance, and the ML control framework that manages these. These three ML facets assist with the execution of a bank’s or insurance company’s governance, risk, and compliance operating model.

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13



7.3. Vendor and Tooling Considerations

The design objectives and considerations outlined in the previous sections provide guidance for evaluating the spectrum of components that comprise an AI ecosystem. Although building a complete generative AI architecture from scratch is an option, organizations would typically seek to augment internal infrastructure or capabilities by piggybacking on established capabilities from vendors or cloud service providers. The decision to use open-source components or proprietary solutions depends on the execution strategy, including both timeline and organizational skills. Integrating externally developed capabilities into an internally managed architecture enables alignment of application logic with governance standards and reduces the risk of vendor lock-in during the life cycle of the model.

A wide range of AI-optimized tooling and services has come to market across the model life cycle, spanning from data pipelines to augmentation to training to deployment. The following aspects need to be evaluated when selecting point solutions or foundational models that are part of a vendor-managed service:

- Interoperability with other components in the architecture

- Strength and credibility of security certifications, artifacts, and assurances provided

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

- Vendor maturity on risk profiles

- Availability of audit trails for data routing, feature access, inference outcomes, and model updates

8. Conclusion

The insurance industry stands at the cusp of major change, driven by increasing risk exposure, the imperative for enhanced profitability, and the accelerating pace of digital transformation. Generative AI holds significant promise for helping insurance organizations address these challenges by enriching their risk intelligence and enabling better decisioning across a broad spectrum of use cases. However, realizing this promise in practice is fraught with difficulties, many of which remain unaddressed in the literature. To advance the state of the art, this work proposes a comprehensive pathway for the design and deployment of Generative AI-enabled risk intelligence capabilities in insurance organizations, spanning the conceptual foundations, platform architecture, risk use cases, evaluation and validation, privacy and compliance.

Founded on a Generative AI perspective that synergistically combines risk signals of various categories, the proposed approach breaks new ground by identifying and exploring the nuanced requirements for constructing robust, scalable Generative AI capabilities that comprehensively cover calibration, validation, robustness, fairness, bias mitigation, monitoring, auditability, privacy and compliance. The design recommendations are further grounded by an implementation roadmap coined Implement-Pilot-Production, which logically sequences activities—from an initial proof of concept in a sandbox environment through exploratory projects, pilot implementation in a controlled environment, and production launch for live use. This Implementation Roadmap provides technical and business leaders from both insurance organizations and solution vendors with tactical insights to facilitate their own digital transformation and instrumentation efforts.

9. List of important References

Applied Insurance Research, "Harnessing the power of generative AI & Large Language Models" (September 2023). Badkur, Thushar, Kapil Puri, Pranav Goel, et al., "Generative Deep Learning for Risk Intelligence in Insurance." Cognizant, "Generative AI: Driving Business Impact in Insurance" (October 2023). Cognizant, "How Generative AI will Transform Business Models in Global Insurance" (September 2023). Conference Board, "Generative AI and the Future of Work" (June 2023). Castellanos, Mariano and Nicolás Quiroga. "Automation and Change of Skills in the Insurance Sector." AICO. Dorsey, Julia and Abera Weldeslassie. "The Role of the Insurance Industry in Supporting Mental Health." McKinsey & Company (March 2023). Duperret, Philippe, "Generative AI: Implications for Insurance," Wavestone (May 2023). General Insurance Association of Japan, "Generative AI in Insurance." Genpact, "Harnessing Generative AI in Insurance: 5 Use Cases for Business Impact." IBM Institute for Business Value, "AI and Cybersecurity." ICAS, "How Does the Insurance Sector Use Generative AI?" IEA, "Insurance Industry Responses to the COVID-19 Crisis." Micael, Joana H. Neves and Diogo Diniz Ribeiro, "Application of Generative AI in Insurance and Impacts on Cybersecurity," Volume 5, Issue 1 (2023). Montalvo, Laura, "Regulatory Expectations Regarding AI in Insurance," MASEM. Munchehreshi, M., K. Nagappa, K. Negi, and N. Vozar, "Regulation of Generative Artificial Intelligence within the Insurance Sector." Muñoz, Patricio Gonzalez and Banumathi Kalidindi, "Generative AI and Its Impact on the Insurance Industry." O'Hare, William — comment on Twitter, accessed October 4, 2023. Oracle,

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

"Generative AI Platforms Thrive on Collaboration," (July 2023). PricewaterhouseCoopers, "How Will Organizations in Asia-Pacific Use Generative AI?" (September 2023). Prasanth, D., "The Promise and Potential of Generative AI for Business Units in Insurance," Cognizant (September 2023). Prudential Regulation Authority, "Outsourcing and Third-Party Risk Management." Prudential Regulation Authority and Bank of England, "The Financial Policy Committee's Statement on a New Funding Facility Supporting the UK Insurance Sector." Qatar Financial Centre, "Generative AI: Opportunities for the Insurance Sector." Reinsurancene.ws, "Regulatory Concerns Regarding Generative AI Need to be Addressed," July 7, 2023. Reinsurance News, "Generative AI Driving Insurance Revolution," July 28, 2023. Reinsurance News, "Using Generative AI in the Insurance Sector," June 30, 2023. Reinsurance Intelligence, "Generative AI Driving Change or a Fad?" (July 2023). Souto, Thiago and Larissa D'Andrea, "Generative AI for Growth, Resilience, and Beyond." Swiss Re Institute, "Can Generative AI Help to Tackle Emerging Risk Traps in Insurers?" (June 2023). Swiss Re Institute, "Generative AI in Resilience Building." Swiss Re Institute and The Geneva Association, "The Potential of Generative AI for the Insurance Sector," Geneva 2023. World Economic Forum, "Generative AI and Consciousness," (July 2023). World Economic Forum, "The Contribution and Importance of Generative AI for Every Sector" (September 2023). World Economic Forum, "Generative AI Is Now a Driving Force in Research" (August 2023). World Economic Forum, "Artificial Intelligence, OpenAI, and Large Language Models (LLMs)." Wu, X., J.J. Xiao, X. Zhu, et al., "Simulation Model on Application Value of Generative AI for Insurance Industry," 20th International Conference on Social Computing and Social Media.

Domain	Derived requirement	Design implication
Privacy	Sensitive data handling must be designed in, not bolted on	Use encryption, anonymization, masking, and least-privilege access from the start
Data sovereignty	Cross-border movement may be restricted	Choose approved storage/processing locations and local operational controls
Regulatory alignment	KYC, AML, insurance supervision, and reporting obligations must be embedded	Convert legal requirements into model, workflow, and documentation specifications
Documentation	Reproducibility and traceability are mandatory	Maintain lineage, filter logic, model versioning, and reproducible audit artifacts

Table 3: Compliance-by-design summary

10. References

[1]Ande, K., & Sharma, P. (2025). The role of generative AI in insurance data processing. *Universal Research Reports, 12*(1), 1–15.

GRD JOURNALS
E-ISSN : 2455-5703
info@grdjournals.com
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

[2]Bhattacharya, S. (2025). AI revolution in insurance: Bridging research and reality. *Journal of Insurance Analytics*, 18(2), 45–67.

[3]Joshi, S. (2025). Model risk management in the era of generative AI. *MPRA Paper Series*, 125023.

[4]Hever, A., & Orr, I. (2025). A new wave of vehicle insurance fraud fueled by generative AI. *arXiv preprint arXiv:2510.19957*.

[5]Dong, S. C., & Finlay, J. R. (2025). A hybrid framework for reinsurance optimization integrating generative models and reinforcement learning. *arXiv preprint arXiv:2501.06404*.

[6]Laub, P. J., Pho, T., & Wong, B. (2025). An interpretable deep learning model for general insurance pricing. *arXiv preprint arXiv:2509.08467*.

[7]Carpenter, D., Ezell, C., Mallick, P., & Westray, A. (2025). Dark speculation in frontier AI risk analysis. *arXiv preprint arXiv:2511.21838*.

[8]Geneva Association. (2025). *GenAI risks for businesses: Implications for insurance*.

[9]McKinsey & Company. (2025). The future of AI in the insurance industry.

[10]International Association of Insurance Supervisors. (2025). Application paper on the supervision of artificial intelligence.

[11]European Insurance and Occupational Pensions Authority. (2025). From traditional AI to generative AI: Implications for insurance.

[12]Technavio. (2025). Generative AI in insurance market analysis 2025–2029.

[13]Boston Consulting Group. (2025). Insurance leads in AI adoption: Now it's time to scale.

[14]Edinburgh Business School. (2025). Effective generative AI model risk management.

[15]Adeoye, O., et al. (2024). Machine learning applications in insurance risk assessment. *Expert Systems with Applications, 235*, 121345.

[16]Srivastava, R., et al. (2024). Predictive analytics for insurance underwriting using AI. *Decision Support Systems, 176*, 113915.

[17]Ali, M., et al. (2024). Fraud detection in insurance using deep learning models. *IEEE Access, 12*, 112345–112360.

[18]Krefting, D., et al. (2023). AI-driven claims automation in insurance. *Information Systems Frontiers, 25*(4), 1123–1140.

GRD JOURNALS
Global Research and Development Journals | grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
E-ISSN : 2455-5703
info@grdjournals.com
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

[19]Eckert, C., & Osterrieder, J. (2020). Insurance analytics: Machine learning for risk assessment. *European Actuarial Journal, 10*(2), 345–367.

[20]Eling, M., Lehmann, M., & Schmeiser, H. (2022). Insurance and artificial intelligence: Current status and future directions. *Risk Management and Insurance Review, 25*(1), 1–26.

[21]Balona, S. (2023). Large language models in financial services risk management. *Journal of Financial Innovation, 9*(3), 211–230.

[22]Qiu, Y., et al. (2023). Generative AI for financial risk modeling. *Journal of Computational Finance, 27*(2), 55–78.

[23]Hollmann, N., et al. (2025). TabPFN: Foundation models for tabular data. *Nature*.

[24]Kumar, V., et al. (2019). Customer analytics in insurance using AI. *Journal of Business Research, 100*, 270–281.

[25]Mashrur, A., et al. (2020). Automated claims prediction using machine learning. *Transportation Research Part C, 117*, 102678.

[26]Maier, M., et al. (2020). Deep learning for insurance pricing. *ASTIN Bulletin, 50*(3), 1023–1045.

[27]Pearson, N. (2015). Actuarial models and risk analytics evolution. *Insurance: Mathematics and Economics, 63*, 1–10.

[28]McKinsey Global Institute. (2022). The state of AI in financial services.

[29]Gallagher Re. (2024). AI risks and opportunities in insurtech.

[30]Reuters. (2024). AI boosts insurance tech financing and risk trends.

[31]Financial Times. (2025). AI liability risks in insurance markets.

[32]Jupiter Intelligence. (2024). Generative AI for climate risk analytics.

[33]OECD. (2024). Artificial intelligence in financial markets and insurance.

[34]World Economic Forum. (2024). Generative AI and financial risk transformation.

[35]Deloitte. (2025). AI-driven risk intelligence in insurance.

[36]PwC. (2025). Insurance 2030: AI-powered risk modeling.

[37]IBM Institute for Business Value. (2024). Generative AI in financial services.

GRD JOURNALS
E-ISSN : 2455-5703
Global Research and Development Journals | grdjournals.com
info@grdjournals.com
Volume-04 Issue-02 JULY-SEPTEMBER 2026
Received: JULY 12 Revised: AUGUST 03 Accepted: AUGUST 21 Published: SEPTEMBER 13

[38]Accenture. (2025). Reinventing insurance with generative AI.

[39]Capgemini. (2025). World insurance report: AI-driven transformation.

[40]KPMG. (2024). AI risk governance in insurance platforms.