AMERICAN ACADEMIC PUBLISHER

INTERNATIONAL JOURNAL OF DATA SCIENCE AND MACHINE LEARNING (ISSN: 2692-5141)

Volume 05, Issue 01, 2025, pages 280-299
Published Date: - 09-06-2025
Doi: -https://doi.org/10.55640/ijdsml-05-01-24

AI-Powered Data Governance for Insurance: A Comparative Tool Evaluation

Shreekant Malviya
Tata Consultancy Services, Plano, Texas, USA

ABSTRACT

As insurers are increasingly utilizing artificial intelligence for underwriting, pricing, and claim processing in an automated manner, end-to-end, open, and industry-level data governance solutions became the top priority. Although numerous AI-driven governance technologies are available, they are mostly purpose-built for generic corporate requirements and do not entirely meet the decision-making-oriented, ethics-conscious, and regulation-compliant insurance industry requirements. This paper presents a comparative evaluation of six top governance platforms—Collibra, Informatica CLAIRE, BigID, Immuta, IBM Watson Knowledge Catalog, and Alation—on eight dimensions, such as explainability, consent management, and insurance-specific flexibility. The research also illustrates the industry specific adoption of AI driven data governance in finance, health care and insurance along with a comparative insight amongst the three most data centric industry. The study reviews insurance governance practices to assess capability gaps in the existing available commercial tools and strategic recommendations to insurers and tech vendors. This paper provides the basis for building AI governance systems that are compatible, scalable, fair, transparent, and flexible to the specific working context of the insurance data universe by overcoming technical limitations and moral dilemmas.

KEYWORDS

AI Governance, Insurance Technology, Data Governance Tools, Decision-Centric Automation, Regulatory Compliance, Ethical AI

1. INTRODUCTION

The insurance sector is undergoing a gigantic digital revolution on the heels of advances in artificial intelligence (AI), data analytics, and cloud computing. AI is being used to apply to core processes such as underwriting, policy tailoring, claims payment, and fraud detection, which had previously been dominated by regulations and human controls [1,2]. Though these innovations hold the promise for insurers of enhanced efficiency, risk sensitivity, and consumer participation, they also present a new crop of governance issues, such as data ethics, algorithmic explainability, and regulatory compliance [3,4].

The crux of such development lies in the question of trust. Therefore, it is required that decisions offered or enabled by AI systems are explainable, understandable, and amenable to analysis compared to those generated by human beings. Insurers' stakes are extremely high. Eligibility, premium, and payments on claims decisions affect policyholders' financial well-being directly. Consequently, insurers are being increasingly pressured by government regulators, industry regulators, and customers to ensure that their AI systems do not only work, but also that they are transparent, fair, and aligned with legal requirements and ethical guidelines [5,6].

In response to these pressures, a number of differing AI-driven data governance systems have evolved. These tools claim to automate policy enforcement, anomaly detection, data lineage monitoring, and consent workflow management. All of these tools, however, have been designed as horizontal corporate solutions, and they are targeted at banking, healthcare, and so on structured data domains. However, these AI-powered data governance platforms are also used in insurance As a result, their capacity to meet the special insurance industry governance requirements of fractured legacy systems, behavior data sources, and context-driven decision-making is largely unproven.

This study aims to address the gap by providing an assessment comparison of top AI-powered data governance platforms in the insurance data ecosystem. It examines the efficiency of such tools in driving key governance features, including metadata control, explainability, consent life cycle monitoring, and regulatory compliance, and capability deficits that are likely to impede their maximum functionality within insurance contexts.

Literature review, industry analysis, and tool-level analysis are applied in the research to identify gaps in current governance tools and invoke a beneficial framework for insurers and vendors to collaborate to formulate open, decision-oriented, and ethically suitable governance frameworks. The result is intended to guide technological strategy and policymaking in AI-based insurance business.

2. METHODOLOGY

The study employs the comparative analysis method shown in **Figure 1**. to liken the landscape of AI-powered data governance solutions and ascertain the prospects for their adoption in the insurance data context. Growth in volumes of data and complexity of data in insurance activities—from underwriting to claims settlement, consumer risk scoring, and reporting to the regulator—make advanced, dynamic, and open governance models a necessity. The general aim of this method is to develop a structured and reproducible model enabling comprehensive comparison of the current tools and suggesting functional gaps, especially in the context of insurance companies' governance requirements. This paper delineates the tool selection, dimension identification, and insight convergence from available data governance principles and industry-specific factors.

The study utilized the qualitative comparative analysis (QCA) method, augmented by thematic dimensioning and interpretative synthesis. Targeted analysis will be directed to address the primary research question: How do current AI-based data governance solutions address the governance, regulation, and operation requirements of the insurance sector? The QCA approach provides a multi-dimensional approach to descriptive and analytical examination of functional capacity across systems. Inferences were made based on publicly accessible material, including white papers, vendor publications, analyst reports, case studies, and peer-reviewed scholarly literature. Multi-source approaches enable both horizontal (cross-tool) and vertical (dimension-specific) analysis and thereby ensure that research includes breadth in addition to depth in analysis.

Data governance tools were selected on three main criteria: explicit integration of machine learning or AI for data governance, application within highly regulated industries like healthcare and finance, and provision of adequate public documentation. Tools that didn't meet these criteria, such as those that didn't have transparency, artificial intelligence, or application in structured data environments, weren't considered. The selection weighed the maturity of the governance feature of each tool against its suitability to be used in actual deployment scenarios, particularly in compliance and risk oversight governed industries such as that of insurance.

All the chosen tools were compared with eight clearly defined properties, based on a mix of industry best practice, regulations, and established standards such as DAMA-DMBOK (Data Management Body of Knowledge) and the NIST AI Risk Management Framework. The indicators are metadata management, data quality management, policy automation, privacy and compliance, explainability and auditability, integration and interoperability, scalability and performance, and insurance-specific adaptation. All in all, these are an integrated definition of good AI-governance.

The addition of explainability and auditability serves the industry's vulnerability to liability and requirement for traceable decision-making, and the insurance-specific flexibility dimension reflects the capability of a tool to perform such activities as fraud detection on claims, risk modeling for underwriting, or consumer protection regulatory affairs. A standard scoring method was created to facilitate comparison analysis.

Each tool was assigned a qualitative rating of 1 to 3 for every dimension, where 3 indicated sophisticated AI-enabled capability, 2 indicated incipient or incomplete capability, and 1 indicated limited or no AI capability. The decision was informed by both explicit evidence, such as technical descriptions and use case examples, and implicit suggestions, such as analyst claims and ecosystem adoption. There was no intention to final rankings but more as heuristic indicators to inform comparison analysis, depict relative strengths, and reveal competence weaknesses. For easier interpretation purposes, results were also shown as radar plots shown in **Figure 3.** and comparative matrices illustrated in **Figure 2**, so stakeholders are able to view which technologies best meet insurance governance strategic requirements.

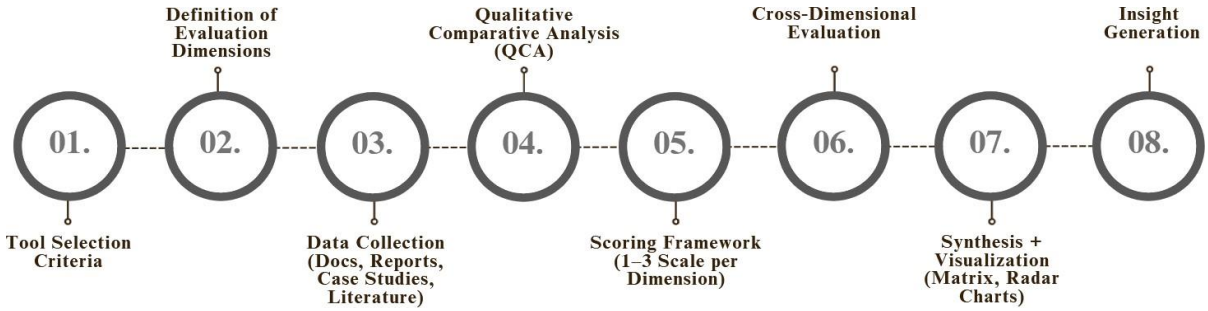

Figure 1: Methodological Framework Flowchart

Data for the research was sourced from a variety of publicly available and verifiable sources consisting of white papers and product documentation from vendors like Collibra, Informatica, BigID, Alation, Immuta, and IBM Watson Knowledge Catalog. Also, benchmark comparisons were obtained from trusted industry reports, such as Gartner's Magic Quadrant for Data Governance and Forrester Wave ratings. Academic knowledge can be established using sources such as IEEE Xplore and SpringerLink, and ACM Digital Library, while implementation-specific knowledge has been established from vendor case studies, YouTube product demonstrations, medium blog posts, and open-source repositories. Information established using public sector websites can include Data.gov and HHS.gov, which can influence insurance-related applications like health claims processing and compliance checks. For source disputes, priority was accorded to peer-reviewed sources or rigorously documented deployments within sectors that are supervised.

Though limited in this method, several boundaries must be noted. The research lacks availability of transparency from each vendor; various proprietary tools underrepresent or conceal implementation detail. Conditions for qualitative scoring scheme, while partially systematic, mandate domains of interpretation which domains can be affected by domains' scope and clarity of supplied documentation. The study further excludes empirical performance benchmarking in operational insurance settings, which could influence the generalizability of certain conclusions. Lastly, the criteria for evaluation, even as they are based on generally accepted frameworks, may not be ideally suited to meet the particular requirements of certain insurance sub-domains, especially those working with unstructured data or underwriting risk in real time. These limitations are well known to ensure methodological transparency and to inform subsequent empirical studies in this discipline.

3. Literature Review

3.1 Foundations of Data Governance

Data governance refers to the systematic alignment of people, process, and technology to make data available, have integrity, be protected, and be used ethically during its lifetime [7]. Proper data governance is very important in highly data-intensive firms, like the insurance sector, whose everyday activities increasingly depend on online portals, predictive analysis, and customer analysis [8, 9,10]. It is a business enabler and regulatory compliance model, that harmonizes usage of data and regulations with business objectives. Insurers must deal with huge amounts of personally identifiable information (PII), policyholder risk information, and third-party information, and therefore governance is a business necessity and not an administrative back-of-house activity.

Governance models historically are founded on proven standards like the DAMA-DMBOK (Data Management Body of Knowledge) that dictates best practices in major functions like metadata management, data quality, stewardship, security, and compliance. [11] Enabling standards like COBIT and ISO/IEC 38505 have also maximized the application of data governance within organizational settings, from systematic control to audit mechanisms and compliance [12]. These principles heavily emphasize formalization of policy, central control, and manual enforcements of measures. Although these maxims have managed organizational data governance for more than a decade, they are considerably less than what is needed today to handle the speed, volume, and variety of the modern digital world [13].

This limitation becomes most evident in the insurance market. With digital transformation, insurers are adopting technologies such as telematics, IoT risk scores, adjusting automated claims, and dynamic pricing, all of which generate fast and diverse data [14,15]. Parallel regulatory testing has grown under regimes such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and future AI rulemaking. These regulatory innovations necessitate operational compliance, transparency, auditability, and real-time responsiveness—capabilities that traditional forms of governance have at times not been able to deliver at scale. The inflexibility of rulebooks and dependence on human interventions place constraints on insurers' capacity to meet operational and regulatory requirements simultaneously [15,16, 17].

Artificial intelligence in data governance frameworks has become strategically relevant in this new landscape. While simple models were historically justifiable, AI verifies them by enabling them to automatically flag data, detect anomalies, enforce dynamic policies, and provide contextual guidance for decisions. AI systems can automatically detect non-compliant data access in near real-time and provide remediation steps for data highlighted [18]. Even so, these advantages are accompanied by new degrees of complexity. The black-box character of open AI models, decision output bias, and inability to trace machine actions into appropriately defined human policies are all serious problems for governance. All of these are particularly relevant in the insurance industry, where data-driven decisions, e.g., accepting or rejecting claims, or underwriting—have both legal and reputational impacts [2,19].

Knowledge of these fundamental traits is necessary in assessing the efficacy and preparedness of AI-based data governance tools. These need to be examined not just in their competence in technology but also in how they can collate and generalize the principles embraced in traditional governance mechanisms. The following section is on the integration of AI technologies into governance practices, with an emphasis on how this technology is particularly suited to respond to evolving governance requirements across regulated sectors like insurance.

3.2 Emergence of AI in Data Governance

Implementation of artificial intelligence into data governance systems is a tremendous step from conventional, rule-based monitoring to responsive, intelligent control systems. This has been brought about by the explosive growth in volume, velocity, and sophistication of data, and increased demand for real-time responsiveness and

high-value regulatory compliance. Traditional governance models, as great as their intellect, will be dependent upon static taxonomies, hand-coded metadata, and predefined sets of rules that lack the type of flexibility needed in today's data world. With organizations under more pressure for operational scale and regulatory adherence, AI was naturally the complementing the efficiency, accuracy, and responsiveness of governance operations [20].

AI technologies now are applied across various levels of governance. One of the first and most significant applications is in automated metadata management, in which machine processes learn to read data in order to infer or create metadata, provenance, and classification. This displaces human cataloging labor and enables immediate updating as information assets change. Anomaly detection methods are used to manage data quality to find anomalies, missing values, and outliers that would otherwise remain hidden in high-volume systems. These technologies employ supervised or unsupervised learning models to scan longitudinally throughout data and trigger alarms on the detection of anomalies [21,22].

In like manner, policy enforcement engines started incorporating natural language processing (NLP) and rule-learning functionality for data policy interpretation and dynamic enforcement—aligning internal guidelines into concordance with access borders, storage durations, and mask protocols as specified by usage contexts. AI takes an active part in handling privacy and consent, especially under regimes like GDPR and CCPA. Product like BigID leverage AI to identify sensitive or personally identifiable information (PII) in structured and unstructured data repositories so organizations can more effectively process data subject access requests (DSARs) and implement consent-based workflows. Explainability tools, generally incorporated into governance platforms, allow audit trails, decision explanation automation, and customer and regulator transparency. This kind of functionality is required in domains such as insurance, where price-, claim-, or fraud-related decision-making has to be reasonable and intelligible [23, 24, 25].

Practical deployments also establish the scope for AI-governance to transform. Some insurance firms have begun implementing AI-based governance solutions to automate fraud detection in the process of making claims. By leveraging historical claim information, geographic patterns, and behavioral anomalies, AI systems can detect fraudulent claims in real-time, creating alerts and initiating examination procedures. This minimizes manual intervention, increases the precision of examinations, and maintains policyholder safeguarding without violating compliance audit guidelines. These solutions prove the practical application of AI-governance solutions when adapted for industry-specific functionality [25, 26, 27].

Some business platforms have sprung into the limelight with this technology. Informatica's CLAIRE engine leverages machine learning to speed up smart metadata discovery, policy recommendations, and predicted data quality profiling. Collibra's AI engine facilitates contextual data discovery and lineage analysis, automating manual stewards. BigID leverages natural language processing and graph-based AI to enable automated data discovery and privacy governance, once more being utilized for regulatory compliance. Although not necessarily created with the insurance sector in mind, they symbolize the application of AI in supporting the creation of more dynamic, responsive, and auditable forms of governance. Research firms like Gartner and Forrester have named the rising strategic relevance of the technologies in regulated industries and project increased utilization in the next five years [28].

However, the application of AI in governance also has intricate challenges. The employment of impassable, "black-box" models may hide policy application reasoning or data classification reasoning, thus making transparency goals government systems wish to maintain outdated. In addition, an increased algorithmic bias risk is being developed, that is, in the analysis of policy domains crossing demographics or behavior data—raising ethical issues in fields like insurance, where information has immediate impacts on consumer outcomes. Excessive dependence on

automation will pose systemic risks, especially if AI systems mis-map critical assets or do not detect instances of regulation breaches. These factors highlight the need for "governance of the governance systems", designing AI mechanisms to be inherently subject to scrutiny, auditable, and ethical fine-tuning [3].

In insurance, the stakes are much higher than that. The increasing dependence of the business on algorithmically driven decisions, i.e., real-time underwriting, auto-adjudication of claims, and behavioral risk modeling—requires intelligent as well as responsible systems of governance, by the business sector. AI governance has the potential for scalable real-time monitoring but without adjustment to the demanding requirements and strong authentication, it can compound underlying governance failures. A review of the performance of these AI technologies across industry sectors provides a critical frame from which to understand their portability and applicability within the insurance data space [2].

This following section explores transferability in AI-powered data governance solutions by contrasting sectoral usage in finance, health care, and insurance, emphasizing best practices, sector-specific challenges, and new lessons for the digital governance revolution of the insurance industry.

3.3 Industry-Specific Adoption of AI-Powered Data Governance

3.3.1 Cross-Sector Benchmarks: AI-Driven Data Governance in Finance and Health Care

Finance and health care are vanguard industries in AI-driven data governance, from which the insurance industry can learn. Both are in high-risk domains characterized by sensitive data and stringent compliance requirements, although with dissimilar approaches driven by their operational contexts.

In finance, AI helps in regulatory compliance of rules such as the Basel Accords, the Dodd-Frank Act, and anti-money laundering (AML) laws through real-time monitoring, auto-categorization, access control, and enhanced auditability. AI is utilized by banks and financial institutions in metadata management, anomaly detection, and dynamic risk profiling through software such as Collibra and IBM Watson Knowledge Catalog [29]. Artificial Intelligence is also at the forefront of Know Your Customer (KYC) and anti-fraud initiatives through transaction behavior and relationship modeling based on graph models. Financial governance solutions, however, are not agile enough to process complicated behavior-based data and extended decision-making timeframes that are present in underwriting and claims payout in the insurance sector [30, 31].

Healthcare has proactive examples of data ethical use, privacy, and contextual consent. Healthcare organizations handle very sensitive data, including EHRs, genomics, and telehealth data, to HIPAA and GDPR requirements. AI products like BigID and Immuta auto-scan for personally identifiable information (PII), propagate consent policies, and enable de-identified data sharing for research. Dynamic policy enforcement and auditable trace paths are pillars of hospital governance, encouraging patients and regulators to trust. Both models contain lessons for insurers, from finance, scalable automation and regulatory precision; and from healthcare, ethical governance and responsive contextualization [32,33].

Governance needs to evolve as insurers bring in wearables and wellness platform data, balancing analytical authority with transparency, equity, and permission. This section discusses the insurance industry's response to such issues and outlines the shortcomings of current implementations in filling the unique governance needs of the industry.

3.3.2 Insurance

Although the insurance industry is a data-driven business by nature, it has trailed banking and healthcare in adopting AI-driven data governance solutions. It has been due to a mix of legacy infrastructure, siloed processes, and historically lenient regulatory environment for compliance. But increasing pressure defined as rising customer demands, changing privacy regulations, and an explosion of alternative data sources—have turned

attention to nimble, intelligent governance frameworks [2].

Insurers work through a complicated policy life cycle, including underwriting, risk assessment, policy issuance, claims settlement, and fraud detection. All of these are increasingly AI-powered with automated underwriting engines, behavioral risk scores through telematics, and predictive triage of claims. But the data governance of the data powering these AI systems is still poor. In contrast to finance's transactional, highly structured data or the standardized clinical data of health care, insurance data tends to be behaviorally contextual, longitudinal, and episodic, resisting rule-based or static governance approaches. Insurance data governance processes today tend to be siloed, business unit–siloed, and tightly coupled to legacy systems [34].

Harmonized consent models, centralized metadata repositories, or real-time enforcement of policies are rarely to be found at the majority of insurers. Consequently, governance is usually reactive, and business-rule enforcement and human monitoring substitute for end-to-end control of data across the entire firm. These constraints disrupt compliance and model stability as well as audit readiness—particularly in high-risk processes such as claims denial or dynamic pricing. Utilization of AI in the insurance space has outpaced the definition of governance processes. As insurance firms launch sophisticated models in underwriting, pricing, and customer interaction, they are increasingly subjected to pressure by regulators and advocacy groups on algorithmic bias, choice transparency, and moral fairness [34].

Governance structures lacking model explainability features, bias auditing, and context transparency lay the insurers open to reputational risk and legal vulnerability. While jurisdictions such as California have begun examining transparency needs surrounding use of AI in insurance, other regulators continue to issue only general guidance, hence propelling the implementation conundrums. On the contrary, several developments are evident. Large insurers have unveiled pilot programs with the introduction of AI within consent-sensitive decision-making and fraud detection systems. UBI products already need policy-sensitive governance structures that manage the gathering, processing, and use of telematics data in risk calculations [35].

In the same way, AI-driven claims sorting systems are now offering audit trails for justifying automated decisions. Yet this technology is generally still compartmentalized to siloed units and lacks an integrated firm-wide interface with back-end governance structures. The governance of insurance is complicated owing to heterogeneity of sources of data and regulation variation by product segments and geographies. In contrast to banking, where compliance is handled in the standardized way, and health care, where ethics are at the center, the business of insurance has to handle risk estimation, consumer transparency, and legal defensibility in parallel. This needs governance infrastructure that can handle a variety of data types—ranging from structured policy data to unstructured claims records, to multimedia evidence, to behavioral activity records—using dynamic, context-sensitive policies.

The insurance sector stands at a crossroads. It possesses the data richness and analytic intent that needs AI-enforced governance but not the architectural and organizational maturation for mass deployments of such technologies. To fill this gap, governance platforms must go beyond their overall capabilities and provide domain-specific modules, for instance, configurable consent engines, explainability architectures, and bias mitigation techniques specific to insurance processes. This chapter combines sectoral data and suggests a comparative schema towards a better analysis of the governance maturity of the insurance sector [36].

3.3.3 Comparative Insight

Cross-industry analysis of AI-driven data governance deployment shows similarities and significant differences in the oversight approaches of finance, healthcare, and insurance in a more automated data environment. Although the three industries work with high-risk data-driven processes, their governance frameworks have different legislative foundations, operational contexts, and ethical issues. These distinctions have profound consequences in

insurance: although learning can be borrowed from other industries, the direct import of tools and frameworks is not enough.

In financial services, the maturity of governance is predominantly determined by regulation coherence. Adherence to regulations like KYC, AML, and Basel-related reporting has prompted early implementation of AI-enhanced solution sets for metadata management, policy automation, and risk-focused alerts. Such solutions are designed for orderly, high-rate data transfers and perform well in a relatively stable regulatory environment. However, their data consistency assumptions and real-time integration of the system tend to overlook the more subtle and episodic patterns of data typical in the insurance sector.

Healthcare, by contrast, is under the influence of a profound ethical framework involving privacy, permission, and patient autonomy. AI-governance in this sector shows mastery of contextual enforcement of privacy, dynamic per missioning, and open data flow—features increasingly applicable to insurance, particularly in health and wellbeing-oriented products. Healthcare technology tends to favor clinical or research compliance over transparency of algorithms in economic decision-making. In insurance, governance stakes are different: not only does decision-reduction occur, but it also generates consequences—such as policy issuances, pricing regimes, or claim payment having both economic and legal effects on people.

Insurance occupies a hybrid terrain, both demanding the regulatory tightness of finance and the ethical responsiveness of healthcare but also possessing its own demands on explainability, fairness measurement, and traceability of decision-making. In comparison to finance, insurance models tend to integrate behavior and context that show great variability among individuals and overtime. In comparison to healthcare, the outputs of AI systems in insurance directly impact customers' access to benefits and exposure to risk of financial loss. These differences pose a governance requirement that is uniquely challenging and remains largely unserved by commercial AI governance systems.

The study also uncovers a deficiency in tooling. Even market leaders such as Collibra, BigID, and Informatica offer end-to-end solutions for data quality, metadata management, and privacy regulation compliance but are not specifically built for insurance-specific processes, e.g., premium justification, dynamic price audits, or consent-based risk assessment. There are a few platforms with pre-built modules to process multimodal data, rules for algorithmic decision-making, or regulatory disclosures around actuarial models and AI-driven claims estimation.

With increasing regulation of AI regulation, such as in the shape of the EU AI Act and state-level state algorithmic fairness law in the U.S., the necessity for sectoral governance solutions increases. Insurers should prioritize configurable, clear, and context-aware technologies over enterprise-wide one-size-fits-all governance platforms to enhance compliance, operational performance, and customer trust.

This comparison analysis will provide the foundation for the study's next stage: a structured analysis of chosen AI-powered data governance systems across eight described dimensions. These dimensions, distilled from industry best practices and the unique requirements of the insurance sector, form a firm platform on which technically valid solutions can be developed that hold corresponding contextual relevance for insurers' current governance challenges.

4. Comparative Evaluation of AI-Powered Data Governance Tools

This part provides systematic comparative analysis of chosen AI-driven data governance systems through literature review and cross-disciplinary ideas. Literature review aims to identify the effectiveness of these tools in meeting general governance requirements and specific insurance data ecosystem requirements. Though there are some platforms with wide governance functionalities, their actual effectiveness in real-world applications, especially in very sensitive, behavioral, and high-risk decision-making data areas such as insurance—usually shows significant

gaps.

The assessment is conducted on eight precisely defined dimensions, laid out in the methodology, such as metadata management, quality of data, automation of policies, privacy and compliance, explainability and auditability, interoperability and integration, scalability and performance, and insurance-specific flexibility. All the products are tested on a qualitative 1 to 3 scale in each category, with the help of publicly available material, case studies, technical whitepapers, and product demonstrations.

The intention behind this comparative review is twofold: one, to contrast the strengths and weaknesses of leading market tools in relation to their AI-governance features; and two, to identify the platforms that are best suited or require improvement to deliver effective and ethical data governance for the insurance sector.

4.1 Evaluation Matrix: AI-Powered Governance Tools

Table 1. provides a comparative matrix assessing five top AI-driven data governance solutions on eight key dimensions. Each dimension represents a key governance capability pertinent to the insurance sector, and each solution was scored on a qualitative 3-point scale:

- 3 – High: Sophisticated AI capacity with high market maturity and industry applicability
- 2 – Moderate: Suitable capability with some restriction or common implementation
- 1 – Low: Non- specialist or limited AI embedding within the dimension Tools Evaluated:

Tools Evaluated:

1. Collibra
2. Informatica CLAIRE
3. BigID
4. Immuta
5. IBM Watson Knowledge Catalog
6. Alation

Alation

Alation is broadly known to be one of the most advanced metadata management and enterprise data cataloging products. Its natural strength is in making data discoverable through search optimization, user interaction, and stewardship interfaces. The platform's user-focused design and robust query-driven discovery have made it a benchmark in numerous large organizations seeking to democratize access to structured data assets.

Relative to industry frontrunners such as Informatica CLAIRE and BigID, Alation is behind in the context of AI-driven governance. Its automated capabilities remain under development, especially where policy enforcement, AI-driven anomaly detection, and dynamic privacy management are concerned. Feature sets such as automatic classification of sensitive data, monitoring of consent, and explainable decision audit trails remain limited or reliant on third-party interfaces.

Alation provides immense value to the insurance sector as a metadata backbone that facilitates the development of controlled, searchable data catalogues and serves as a basis for managing data. Nevertheless, its limited AI integration keeps it out of the scope of being applied as an independent governance solution in scenarios requiring explainability, risk-scoring transparency, or automated regulatory compliance. Its present application is most appropriately considered as an adjunct to AI-oriented platforms, rather than as a stand-alone system for managing high-risk decision-making situations [29, 37, 38, 39, 40, 41, 42].

Table 1: Comparative Evaluation of Governance Tools

Tool / Dimension	Metadata Mgmt	Data Quality	Policy Automation	Privacy & Compliance	Explainability & Auditability	Integration & Interoperability	Scalability & Performance	Insurance - Specific Adaptability
Collibra	3	2	3	2	2	3	3	2
Informatica CLAIRE	3	3	3	2	2	2	3	2
BigID	2	2	2	3	3	2	2	2
Immuta	2	2	3	3	2	2	2	1
IBM Watson Knowledge Catalog	2	2	2	2	2	3	3	1
Alation	3	2	1	1	1	3	2	1

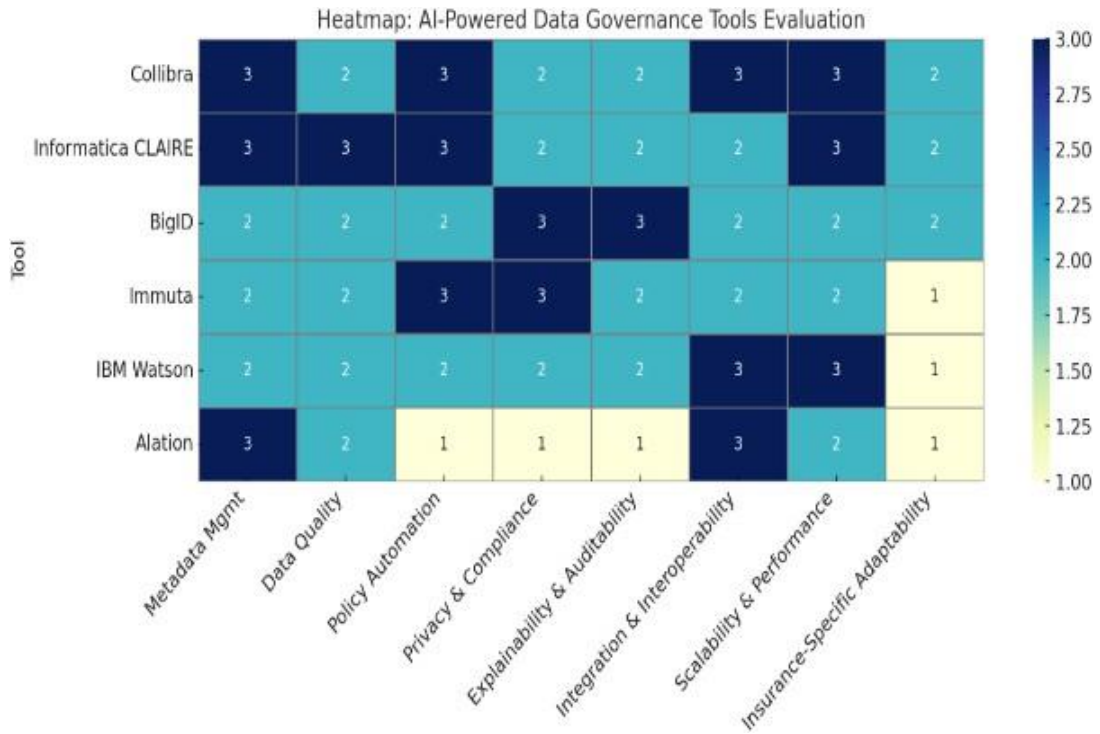

Figure 2. Heatmap plot of qualitative scores (1–3 scale) given to six governance platforms across key dimensions. Darker is better for functional maturity. The plot indicates general underperformance in explainability, fairness auditing, and insurance-specific functionality, while comparative prowess in metadata management and policy automation prevails.

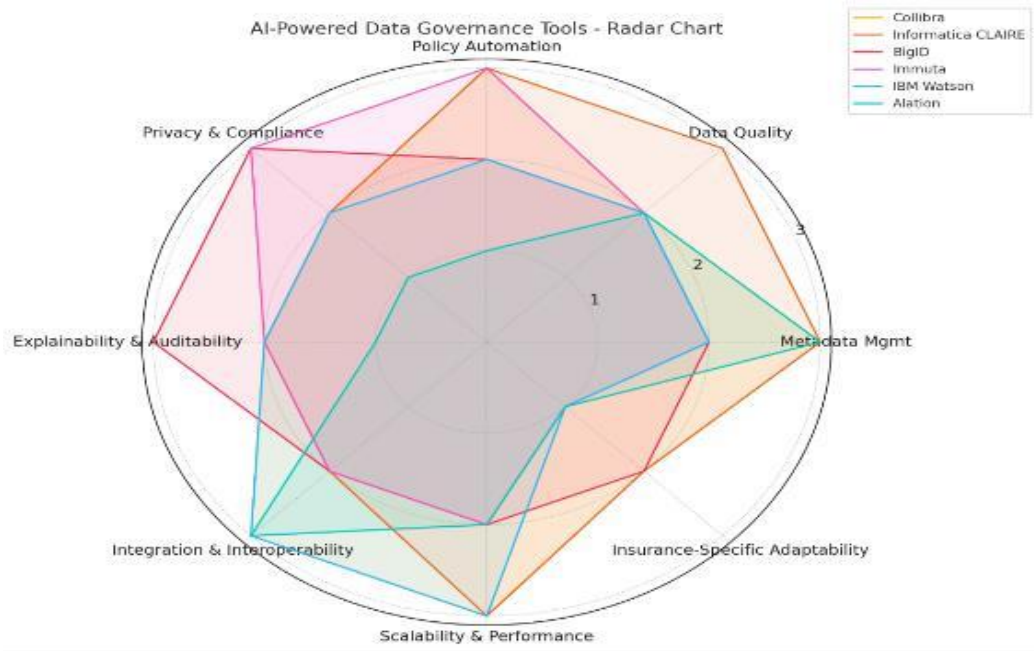

Figure 3. Radar chart showing relative performance of six AI-powered data governance platforms against eleven test parameters. While Collibra and Informatica CLAIRE platforms have high metadata management and scalability, all of those that were tested have medium insurance-specific flexibility and explainability capability and show an across-the-board lack of decision-centric governance across the industry.

5. Gap Analysis and Discussion

5.1 Interpretation of Tool Performance in the Insurance Context

The comparison grid indicates that data governance platforms powered by AI are typically mature in enterprise-wide capabilities but lag behind for the insurance industry's specialized governance needs. Collibra and Informatica CLAIRE lead in metadata management, policy automation, and scalability capabilities extremely useful for highly structured and centralized environments like banking or enterprise IT. But such systems are far short of satisfying the unique needs of insurance operations, especially where decisions have fiscal, ethical, or regulatory implications.

The key insurance requirement is neither data cataloging nor access control but the processing of algorithmically-computed decisions like price, claims acceptance, and risk rating through transparent, explainable, and audit-ready procedures. Although Immuta and BigID both have solid consent and privacy, they have no native transparency underwriting justification capabilities and traceability capabilities in claims handling.

Figure 2. and **Figure 3.** pinpoint the trend unmistakably: although all the solutions are excellent on business functionality, they fall short by far on explainability, permission traceability, and insurance adaptation. These are not secondary considerations; these are issues of equitable and legitimate decision-making in insurance.

This evaluation reaches a critical conclusion: AI governance toolsets at present are crafted for information environments, rather than decision environments such as insurance. Their incompatibility with the operational reality of insurers weakens their capacity to support safe, scalable, and ethical AI uptake in this sector.

5.2 Cross-Dimensional Gaps in Insurance Governance Needs

Multiple systemic governance deficiencies are evident throughout the platforms reviewed—deficiencies that are important matters to the insurance market considering its dependence on data-driven, high-stakes decision-making.

There is an enormous deficit of explainability and auditability. While regulatory burdens are increasing and customers are increasingly demanding visibility, there are very few technologies with inherent facilities to track the thought process behind AI-driven policy pricing or claim settlement decisions. In the absence of such modules, insurers remain vulnerable to regulatory investigations, litigation, and reputation loss when decisions cannot be explained in plain terms.

The second primary shortfall is insurance-specific agility. In contrast with other industries, the insurance industry is based on multimodal data, which consists of structured policy documents, unstructured claims notes, sensor observations, and behavioral logs. Current governance products are not logic- or module-pre-configured to address heterogeneous and context-aware data streams, or dynamic policies at the point of decision.

Consent traceability is also a concern. In insurance products like UBI, consent evolves and changes along policy terms and channels. Most models fail at static models of access control short of the complexity and time-related nature of actual mobile-focused and IoT-enabled insurance product consent requirements.

Finally, integration with the legacy infrastructure is still a technical and operational issue. Insurers tend to operate on-decades-old-deployment-decades-fragmented systems, and governance solutions that are not backward compatible, modularly integrable, or hybrid cloud-deployable modes are difficult to scale.

The inter-disciplinary gulfs suggest an even more profound problem: current systems are great at handling data but are not engineered to cope with the choice logic of sophisticated, regulated, and bespoke flows. For insurers, this is not a competitive advantage issue, it is a strategic risk that will hold back the proper adoption of AI, infuriate regulation, and erode policyholder trust.

5.3 Ethical and Regulatory Implications

The deficiency seen in AI-based data governance solutions is not merely technical; they have profound ethical and regulatory consequences for the insurance industry. As insurers increasingly use AI models to automate underwriting, pricing, and claims determinations, the absence of consolidated governance systems threatens fairness, transparency, and accountability.

One of the most relevant concerns is algorithmic bias. Lacking fairness auditing or bias detection functionality built into the platform, governance platforms may facilitate opaque models that return results disproportionately affecting covered populations. In the case of insurance, this may result in increased premiums, tardy payments, or denial of coverage based on correlated but legally justifying characteristics—exacerbating significant compliance issues under anti-discrimination statute and eroding trust among consumers.

The shortage of an explainability infrastructure is no less urgent. As governments enact AI transparency legislation such as the EU AI Act and other U.S. state bills, insurers must make transparent the logic of algorithmically driven decisions. This includes specifying the data input employed, managing consent, and policy rules affecting the decision. The majority of solutions today do not have native capability for lineage tracing, creating both legal risk and operational risk.

The lack of traceability of granular permissions lowers insurers' capacity to maintain changing privacy rights. Under usage-based or wellness-included insurance plans, policyholder data may still be employed downstream even after the revocation of consent, hence putting regulatory non-conformity to GDPR, CCPA, or particular state-level privacy legislation at risk. These frailties underscore the limitations of static access controls within a scenario were data

usage must be controlled contextually and in real-time.

This leads to an increasing ethical power imbalance. Consumers tend to be badly informed about the utilization of their own or behavioral data, about risk calculation methods, or about the rationale of premium or claim decisions. In the absence of open governance processes, insurers expose themselves not only to damage of their reputation, but also to loss of their moral legitimacy to operate in data-driven product markets.

In the context of the accelerating rate of legal innovation and moral demands, governance methods must mature to provide explainable, consent-sensitive, and bias-aware AI—features that should be must-haves and not nice-to-haves in insurance data environments.

5.4 Root Causes of Governance Gaps

The disparity between current AI governance tools and the unique requirements of the insurance sector is the result of a combination of structural and systemic reasons—both within the tool design as well as in the operational culture of the business.

Foremost among them, most governance technologies on the commercial market are horizontal enterprise solutions. Designed to be sector-agnostic, they address universal functions such as metadata classification, access rights, and static compliance verification. Useful as these functions certainly are, they are not enough for industries such as insurance, where governance also needs to oversee risk-based, personalized, and decision-driven operations. The absence of verticalization indicates a significant deficiency in product design: governance platforms have yet to be adapted to insurance-specific use cases, including underwriting rule elucidation, premium rationale analysis, and multi-party data exchange in reinsurance agreements.

Secondly, the governance software market has traditionally focused more on data management and privacy compliance than on decision oversight in real time. Most solutions, for instance, were developed in response to the needs of finance and healthcare, where governance involved safeguarding structured data and ensuring research ethics. In comparison, insurance demands governance systems that have the capacity to oversee algorithmic logic, adjust policy rules, and review behavioral scoring models, which are the specialty of existing platforms.

Third, implementation challenges persist due to aging infrastructure. Insurers typically possess legacy policy admin systems, fragmented customer data repositories, and mainframe-based claims systems. These do not expose modern APIs, standard formats, and modular architecture to easily integrate governance tools. Consequently, insurers experience deployment lag, partial coverage, and operational drag in trying to implement end-to-end governance.

Fourth, there is also a chronic absence of cross-functional ownership of governance. Actuaries, underwriters, data scientists, and compliance officers frequently operate in silos with no shared standards for model use governance, data consent, or explainability. This generates disjointed efforts, spotty application of regulations, and missed opportunities for consistency of governance across the AI lifecycle.

Last but not least, regulatory uncertainty hinders innovation. Insurers in most jurisdictions lack clear guidance on what is adequate AI transparency and fairness. In the absence of detailed regulations, both suppliers and insurers hold back investment in sophisticated governance capabilities. That creates a culture of reactive compliance instead of proactive risk management, and insurers are ill-equipped for when regulators do come knocking in the future.

These fundamental issues collectively create a high-friction environment where governance mechanisms are weak, insurers lack resources, and regulations are outpacing the speed of business. To close this governance gap demands more sophisticated tools, joint disciplinary coordination, modular platform architecture, and forward-thinking regulatory policies—topics to which we now turn.

5.5 Strategic Risk to the Insurance Industry

The gap between existing AI governance technologies and the insurance sector's unique needs is a nascent strategic risk. As insurers hasten the integration of AI into operations at the core—underwriting, pricing, risk modeling, and claims—they increase their dependence on algorithmic decisions often black-boxed, uninterpretable, and unbundled.

This generates stacked and aggregated risks:

- **Regulatory Risk:** New legislation, including the EU AI Act, U.S. state transparency laws, and shifting notions of fairness relevant to insurance are quickly increasing the bar for algorithmic accountability. Insurers without traceability of decisions, bias protection, or sharing of consent will be exposed to greater risks of audit, penalties, or operational constraint.
- **Operational Risk:** Inconsistent governance leads to discrepancies in decision-making between channels, raising the risk of price variation, unwarranted claim rejection, or regulatory non-compliance. All these are opposite to operational efficiency and lead to internal bottlenecks.
- **Reputational Risk:** With the era of increased data sensitivity, public outcry due to unjust or unfathomable behavior—especially that against vulnerable customers—can lead to legal proceedings, bad press, and customer loss. Transparency is rapidly becoming a differentiator.
- **Innovation Risk:** Without strong governance, insurers may be incapable of developing new data products—like usage-based insurance, AI-powered fraud detection, or customized policy packages. Governance unpreparedness can cause the pace of innovation to erode, constraining long-term competitiveness.

Data governance, in this respect, has exited the back office. It is a strategic catalyst of responsible AI and essential to sustainable innovation, regulatory resilience, and market leadership.

5.6 Bridging the Governance Gap

Closing the governance gap is not a matter of a simple refresh of technologies; it is a matter of transforming platform design, organizational coordination, regulation alignment, and governance philosophy fundamentally. From the analysis and cross-industry comparison, the six below recommended strategies can help bridge the gap:

1. Verticalization of Governance Platforms

Vendors should build insurance-intelligent modules that are particularly designed for critical decisioning processes like claim adjudication transparency, price explanation, and actuarial governance. Tools shall have to move from horizontal compliance to domain-specific policy understanding, possibly via APIs that talk to actuarial models, claims systems, or underwriting engines.

2. Modular and Interoperable Architecture

Due to legacy problems within insurance IT systems, governance tools should be of modular, plug-and-play architecture with open APIs and loose connections. This allows insurers to adopt incrementally while preserving backward compatibility and data integrity.

3. Decision-Centric Governance Models

Tools should be advanced in order to facilitate governance of decisions rather than governance of data. This includes:

- Model audit trails and transparency of logic
- Inline equity analysis
- Automated policy-based gating of decisions

These functionalities must be intrinsic, not adjunctive, in order to enable real-time, auditable, and defendable use of AI.

4. Cross-Functional Governance Councils

Insurers must establish governance by forming permanent, cross-disciplinary boards comprising data scientists, legal experts, underwriters, actuaries, and business stakeholders. They must also develop and implement AI usage policies, fairness measures, and explainability standards and thereby close the gap between governance, enterprise risk management, and ethical governance.

5. Proactive Regulatory Collaboration

Insurance firms need to collaborate with regulators and industry bodies in order to shape domain specific governance standards, particularly in the case of automated decision-making and explainability. Collaborative policy framework design can pilot test feasibility, intelligibility, and compliance fit prior to enforcement obligations being made mandatory.

6. Ethical Governance by Design

Insurers must embed ethical AI principles into their governance framework, including compliance. This involves:

- Designing human-in-the-loop review of decisions
- Enforcement of withdrawing consent
- Explainability to consumers
- Counterfactual fairness assessment

These design elements establish trust, minimize harm, and give insurers a strong foundation for responding to changing consumer expectations. By implementing these strategies, insurers are able to shift governance from a compliance point to a strategic asset that fosters innovation, facilitates regulatory goodwill, and maintains public trust in the era of algorithms.

6. Recommendations

6.1 Summary of Key Gaps and Needs

The comparative study indicates persistent and systematic divergence between the design requirements of current AI-enabled data governance technology and operational governance requirements of the insurance sector. While certain platforms have evolved mature aspects in metadata management and rule compliance, they are deprived of providing domain-knowledge-wise expertise required in governance of sophisticated, high-value, and decision-making insurance operations.

One such flaw is the lack of an explainability framework. The majority of the technologies lack inherent capabilities to track and safeguard algorithmic decisions within the framework of underwriting, risk management, or claims adjustment. The absence of transparency is an immediate deflection of new regulatory requirements as well as in-house compliance needs, making insurers susceptible to audit failure, legal risk, and reputation loss.

Consent lifecycle management is equally underdeveloped. A life insurance company that starts to hold progressively more behavior and biometric data from wearables, telematics, and mobile applications must capture consent as it is required, requested, and withdrawn dynamically through time, across systems, and between partners. Static role-based access models of governance are unable to keep up with delivering the fluidity and granularity needed for stewardship of data in highly personalized insurance products.

The third critical gap is bias and fairness testing. As more platforms use machine learning algorithms to forecast eligibility, price, and risk, few platforms give insurers operational tools to identify algorithmic bias, monitor

fairness metrics or conduct counterfactual analysis. This lack leaves insurers open to regulatory sanction and discriminatory outcome issues.

The pervasive nature of walled and legacy systems within insurance contexts is an existence integration dilemma. Most governance solutions take for granted interoperable, cloud-native data models. Inability to provide modular connectivity, API-level agility, or hybrid deployment support tends to hamper implementation and limit usability within current insurance technology infrastructures.

These limitations are not only individual technical structural deficiencies but connected structural deficits which, taken collectively, weaken insurers' capacity to employ AI in an open, compliant, and ethically justifiable manner.

6.2 Strategic Recommendations for Insurers

To meet these governance needs, insurers must embrace an integrated approach with technology procurement, organizational setup, ethical policy formulation, and future-oriented regulation.

Insurers would have special governance departments at the organizational level that include actuarial, compliance, product, legal, and data science functions. These cross-functional units would have to be accountable to formulate organization-wide policy on AI governance, establish suitably limiting model risk, and audit algorithms for accuracy, transparency, audibility, and fairness. Baking governance into organization risk and ethics frameworks will be of greatest consequence in ensuring accountability.

There is a need for insurers to be concerned with governance platforms that support decision-focused governance, where datasets are managed in addition to tracing the rationale behind the AI system output. Platforms should possess inherent model lineage monitoring capabilities, integrated explainability modules, and real-time audit logs. Where current tools are deficient in such functionality, insurers can utilize governance wrappers or middleware—mid-layer software observing and following the output of black-box AI models—to exhibit enhanced traceability and to govern decision outputs without needing complete retraining or model replacement.

Insurers must work with their vendors to co-develop insurance-specific extensions to real-world product and policy semantics, and in this way, render the platform more relevant. These can involve template-based regulation for underwriting rules, actuarial pricing justification, and claims adjudication. Procurement groups must assess tools not just on technical requirements but also with regard to correspondence with operational policy sophistication and the insurer's regulatory risk environment setting.

Ethically, regulation should be created in the form of internal AI usage charters prescribing minimum standards for explainability, customer transparency, fairness enforcement, and human-in-the-loop monitoring. Such regulations should be formulated through pre-deployment governance processes like fairness checks, sensitivity studies, model documentation, and audit readiness checks.

Insurers must shift from passive regulatory conformists to proactive regulatory participants. By participating in regulatory sandboxes, industry norms, and involvement in institutions of policy development, insurers can influence governance requirements that are fit and effective to implement—thereby minimizing the likelihood of breakdown in compliance and post-deployment testing.

Through taking such strategic turns, insurers will be answering mounting calls for responsible regulation of AI and establishing a platform of resilience and trust upon which to build long-term competitiveness in an insurance economy based on data.

6.3 Vendor and Ecosystem-Level Recommendations

Insurers themselves need to provide AI governance, but the wider ecosystem—technology suppliers and regulators in particular—will have to take a crucial role in making it possible. Governance technologies today, while good in

most corporate settings, tend not to be imbued with the custom-tuned intelligence and agility necessary to tackle decision-making problems specific to the insurance domain. In order to bridge the gap, vendors have to make their offerings more customized, and the ecosystem must facilitate the work on collaborative standards.

First, the vendors must make investments in vertical integration of their solutions within the insurance space. This includes the creation of pre-configured modules of governance for imposition of actuarial regulations, premium justification audits, traceability of risk models, and transparency of claims adjudication. These modules must be capable of capturing both regulatory intricacy of insurance as well as variability of data and sensitivity of decision-making. Vendor roadmaps should have explainability and bias-detection capabilities high on their agenda as baseline requirements, rather than present them as add-ons or integrations.

Secondly, platforms must support plug-and-play interoperability. Most insurers cannot go all the way to cloud-native designs. Thus, technology for governance must support low-code connectors, hybrid deployment capabilities, and policy APIs that allow integration of legacy and newer systems. This flexibility in architecture must be present to do transformation incrementally and implementation with risk management.

Third, the ecosystem must generate collective compliance artifacts that facilitate audit-readiness and regulatory harmonization. These can be such things as standardized model cards, consent receipts, data usage declarations, and audit logs specific to insurance processes. These artifacts must be collaboratively developed by vendors, regulators, and insurance coalitions to be legal and feasible for operations.

Fourth, insurers and technology companies should engage with regulatory innovation vehicles, like sandboxes, safe harbors, or industry working groups. These platforms allow for experimentation with AI governance policy by doing, reveal areas where tools are lacking, and speeding synchronization of governance norms across jurisdictions.

Insurers should promote the use of governance standards in business reviews like ISO certifications or NAIC solvency exams. Identifying governance maturity as an element of operational resilience would encourage vendors and insurers to spend money on scalable, ethical, and industry-specific governance processes.

By matching vendor competency with the requirements of the insurance sector and enabling comprehensive coordination across the ecosystem, the sector can shift away from siloed compliance into an integrated, responsive, and responsibly driven governance framework.

7. CONCLUSION

This study has introduced a formalized and comprehensive analysis of AI-driven data governance platforms with focus on the operational and ethical issues of the insurance data marketplace. A review of six platforms in eight domains of governance, supplemented with finance, healthcare, and insurance adoption trend studies, indicates that existing tools, advanced as they are at general-purpose data management, fall short in meeting the decision-priority requirements of today's insurance companies.

Study discovers a common denominator: static compliance and access control, and metadata automation tools alone are not sufficient to solve information and algorithmically intensive judgments essential in underwriting, claims, and pricing. Current platforms do not have necessary depth and speed of explainability, fairness auditing, consent lifecycle management, and legacy system integration, which are crucial for insurers operating within complex regulatory landscapes.

The report offered practical recommendations to rectify the above imbalances at both insurer and ecosystem levels. This encompasses inter-disciplinary governance platform development, deployment of solution flexibility, incorporation of moral governance models, and interaction with regulation. A tailored governance framework offers insurers a concrete framework to depart from reactive compliant to proactive, open, and responsive AI governance.

As the insurance industry becomes increasingly dependent on AI for better performance, tailored solutions, and risk management, governance must take priority. It must become a strategic imperative—regulated not just to empower authorities but to ensure fairness, facilitate accountability, and enhance policyholder confidence.

Follow-up research must confront this paradigm with empirical tests in real insurance settings, measure human emotions against AI-driven decisions, and identify applications of new technologies such as blockchain and federated learning that enhance privacy, transparency, and control. Multidisciplinary research must anchor technological progress on ethical, legal, and social foundations.

In a trust-based insurance business, insurance companies may not be in a position to have systems closed. AI can perform well only in its function if its decisions are not just fast and scalable but also just and transparent. That is the equation this research makes possible—to innovate wisely, to regulate justly, and to lead courageously in the age of intelligent automation.

REFERENCES

1. "Impact of AI in the General Insurance underwriting factors," Central European Management Journal, 2023, doi: 10.57030/23364890.cemj.31.2.72.
2. S. Bhattacharya, G. Castignani, L. Masello, and B. Sheehan, "AI revolution in insurance: bridging research and reality," Front Artif Intell, vol. 8, p. 1568266, Apr. 2025, doi: 10.3389/frai.2025.1568266.
3. J. Onoja, O. Hamza, A. Collins, A. Eweja, A. Daraojimba, and A. Pub, "Digital Transformation and Data Governance: Strategies for Regulatory Compliance and Secure AI-Driven Business Operations," Journal of Frontiers in Multidisciplinary Research, vol. 02, pp. 43–55, Jan. 2021, doi: 10.54660/.IJFMR.2021.2.1.43-55.
4. V. M. Aragani, "Revolutionizing Insurance Through AI and Data Analytics: Innovating Policy Underwriting and Claims Management for the Digital Era," FTSCL, vol. 2, no. 3, pp. 176–185, Sep. 2024, doi: 10.69888/FTSCL.2024.000243.
5. Q. V. Liao and S. S. Sundar, "Designing for Responsible Trust in AI Systems: A Communication Perspective," 2022, doi: 10.48550/ARXIV.2204.13828.
6. N. Balasubramaniam, M. Kauppinen, A. Rannisto, K. Hiekkanen, and S. Kujala, "Transparency and explainability of AI systems: From ethical guidelines to requirements," Information and Software Technology, vol. 159, p. 107197, Jul. 2023, doi: 10.1016/j.infsof.2023.107197.
7. R. Abraham, J. Schneider, and J. Vom Brocke, "Data governance: A conceptual framework, structured review, and research agenda," International Journal of Information Management, vol. 49, pp. 424–438, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.07.008.
8. M. R. Haque, "Data-Driven Risk Assessment in Insurance Underwriting: Evaluating the Ethical and Economic Trade-offs of AI-Powered Actuarial Models," Frontline Learning Research, vol. 05, p. 30, Mar. 2025, doi: 10.37547/marketing-fmmej-05-03-02.
9. E. Owens, B. Sheehan, M. Mullins, M. Cunneen, J. Ressel, and G. Castignani, "Explainable Artificial Intelligence (XAI) in Insurance," Risks, vol. 10, no. 12, Art. no. 12, Dec. 2022, doi: 10.3390/risks10120230.
10. Regulation of Artificial Intelligence in Insurance: Balancing consumer protection and innovation," The Geneva Association. Accessed: May 20, 2025. [Online]. Available: https://www.genevaassociation.org/publication/public-policy-and-regulation/regulation-artificial-intelligence-insurance-balancing
11. S. Earley, D. Henderson, and Data Management Association, Eds., DAMA-DMBOK: data management body of knowledge, 2nd edition. Basking Ridge, New Jersey: Technics Publications, 2017.

12. "ISO/IEC 38505-1:2017," ISO. Accessed: May 27, 2025. [Online]. Available: https://www.iso.org/standard/56639.html

13. F. Yaqoob, "Data Governance in the Era of Big Data: Challenges and Solutions," Oct. 2022, doi: 10.5281/ZENODO.8415833.

14. Praveen Kumar Koppanati, "Leveraging Telematics and IoT for Usage-Based Insurance Models," Oct. 2024, doi: 10.5281/ZENODO.13912578.

15. F. V. den Boom, "Regulating Telematics Insurance – Enabling Car Data-Driven Innovations," European Business Law Review, vol. 34, no. 1, Jan. 2023, Accessed: May 17, 2025. [Online]. Available: https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\EULR\EULR2023013.pdf

16. M. Jacobs, "AI Revolution in Insurance: Opportunities and Legal Pitfalls," Insurance Journal. Accessed: May 27, 2025. [Online]. Available: https://www.insurancejournal.com/magazines/mag-features/2024/11/18/801366.htm

17. European Parliament. Directorate General for Parliamentary Research Services., The impact of the general data protection regulation on artificial intelligence. LU: Publications Office, 2020. Accessed: May 27, 2025. [Online]. Available: https://data.europa.eu/doi/10.2861/293

18. S. Tewari, "AI Powered Data Governance - Ensuring Data Quality and Compliance in the Era of Big Data," JAIGS, vol. 8, no. 1, pp. 187–197, May 2025, doi: 10.60087/jaigs.v8i1.364.

19. "Black box AI: Unveiling the risks of uninterpretable models." Accessed: May 27, 2025. [Online]. Available: https://www.businessthink.unsw.edu.au/articles/black-box-AI-models-bias-interpretability

20. A. Groll, A. Khanna, and L. Zeldin, "A Machine Learning-based Anomaly Detection Framework in Life Insurance Contracts," Nov. 26, 2024, arXiv: arXiv:2411.17495. doi: 10.48550/arXiv.2411.17495.

21. D. Oyighan, E. S. Ukubeyinje, B. T. David -West, and B. D. Oladokun, "The Role of AI in Transforming Metadata Management: Insights on Challenges, Opportunities, and Emerging Trends," AJIST, vol. 14, no. 2, pp. 20–26, Sep. 2024, doi: 10.70112/ajist-2024.14.2.4277.

22. S. Iseal and M. Halli, "AI-Powered Fraud Detection in Digital Payment Systems: Leveraging Machine Learning for Real-Time Risk Assessment," Feb. 05, 2025, Computer Science and Mathematics. doi: 10.20944/preprints202502.0278.v1.

23. "Utilizing Artificial Intelligence (AI) in Healthcare Insurance to Transform Risk Assessment, Claims Processing, and Fraud Detection - ISJEM Journal." Accessed: May 20, 2025. [Online]. Available: https://isjem.com/download/utilizing-artificial-intelligence-ai-in-healthcare-insurance-to-transform-risk-assessment-claims-processing-and-fraud-detection/

24. A. Gour, "AI-based Natural Language Processing (NLP) Systems," JOURNAL OF ALGEBRAIC STATISTICS, vol. 11, no. 1, Art. no. 1, Dec. 2020.

25. S. Pamarthi, "AI Meets Anonymity: How named entity recognition is redefining data privacy," World Journal of Advanced Research and Reviews, vol. 22, no. 1, pp. 2045–2053, 2024, doi: 10.30574/wjarr.2024.22.1.1270.

26. L. Pandiri and S. Chitta, "Leveraging AI and Big Data for Real-Time Risk Profiling and Claims Processing: A Case Study on Usage-Based Auto Insurance," KS, 2022, doi: 10.53555/ks.v10i2.3760.

27. B. Sudabathula, "Revolutionizing Insurance: The Impact of AI on Claims Processing," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 1, Art. no. 1, Feb. 2025, doi: 10.32628/CSEIT251112302.

28. P. Matai, "The Imperative of AI Governance: Steering BFSI towards Responsible Innovation," Journal of Artificial Intelligence & Cloud Computing, pp. 1–5, Feb. 2024, doi: 10.47363/JAICC/2024(3)319.

29. M. Cherradi, F. Bouhafer, and A. EL Haddadi, "Data lake governance using IBM-Watson knowledge catalog," Scientific African, vol. 21, p. e01854, Sep. 2023, doi: 10.1016/j.sciaf.2023.e01854.

30. K. Koçar, "AI-based Decision Making Process in the Finance Sector," Next Generation Journal for The Young Researchers, vol. 8, no. 1, pp. 143–143, Dec. 2024, doi: 10.62802/rz706w81.

31. "A review article: -the Growing Role of Data Science and AI in Banking and Finance," IRJMETS, Aug. 2023, doi: 10.56726/IRJMETS44000.

32. C. Lawrence, P. Seth Dobrin, P. Gil Alterovitz, Y. Schlesinger, and M. D. Chornenky, "AI Governance in Healthcare: Best Practices, Solutions, and Unresolved Issues," Telehealth and Medicine Today, vol. 9, no. 4, Art. no. 4, Aug. 2024, doi: 10.30953/thmt.v9.521.

33. S. Neupane, S. Mittal, and S. Rahimi, "Towards a HIPAA Compliant Agentic AI System in Healthcare," May 06, 2025, arXiv: arXiv:2504.17669. doi: 10.48550/arXiv.2504.17669.

34. M. Eling, I. Gemmo, D. Guxha, and H. Schmeiser, "Big data, risk classification, and privacy in insurance markets," Geneva Risk Insur Rev, vol. 49, no. 1, pp. 75–126, Mar. 2024, doi: 10.1057/s10713-024-00098-5.

35. "Geneva Association report lays out key considerations to ensure AI regulation in insurance protects customers without compromising innovation," The Geneva Association. Accessed: May 27, 2025. [Online]. Available: https://www.genevaassociation.org/press-releases/geneva-association-report-lays-out-key-considerations-ensure-ai-regulation-insurance

36. "How insurers can leverage the power of generative AI US – Municipio Camargo." Accessed: May 20, 2025. [Online]. Available: https://municipiocamargo.gob.mx/uncategorized/how-insurers-can-leverage-the-power-of-generative/

37. "Introducing CLAIRE GPT The Future of Data Management | Informatica." Accessed: May 20, 2025. [Online]. Available: https://www.informatica.com/blogs/introducing-claire-gpt-the-future-of-data-management.html

38. B. R. Nida, "Bridging Process Intelligence, Data Management, And Governance: A Unified Approach with SAP Signavio, SAP Datasphere, And Collibra," JFMR, vol. 5, no. 2, pp. 69–74, 2024, doi: 10.54660/.IJFMR.2024.5.2.69-74.

39. "AI Security & Governance," BigID. Accessed: May 20, 2025. [Online]. Available: https://bigid.com/ai-security-governance/

40. H. Devane, "Immuta AI: Data Provisioning at the Speed and Scale of AI," Immuta. Accessed: May 20, 2025. [Online]. Available: https://www.immuta.com/blog/immuta-ai-announcement/

41. "Why Data Governance is Essential for the Insurance Industry | Alation." Accessed: May 17, 2025. [Online]. Available: https://www.alation.com/blog/data-governance-in-insurance/

42. "The Importance of Data Governance for AI: Ensuring Trustworthy AI Systems | Alation." Accessed: May 20, 2025. [Online]. Available: https://www.alation.com/blog/importance-data-governance-ai/