



How to build a data strategy & data strategy for insurance companies

2025 -2026

By Salvatore Magnone,
sal.magnone@door3.com

DOOR3
Labs

How to Build a Data Strategy & Data Strategy for Insurance Companies

By Salvatore Magnone

<https://www.linkedin.com/in/salmagnone/>

For DOOR3 Business Applications

<https://www.door3.com/>

How to Build a Data Strategy

In today's business environment, data has become a critical asset that can drive competitive advantage, operational efficiency, and strategic decision-making. However, many organizations struggle with fragmented data initiatives that lack coherent direction. Building a comprehensive data strategy requires a systematic approach that aligns with broader organizational objectives while enabling future capabilities.

Start with Organizational Strategy Alignment

Your data strategy cannot exist in isolation. It must be fundamentally anchored to your organization's strategic priorities, business objectives, and operational, regulatory, and compliance requirements. This alignment ensures that data initiatives directly support revenue generation, cost reduction, risk mitigation, or whatever key performance indicators drive your business forward.

Begin by identifying how data can enable your organization's strategic goals. If your company is focused on customer acquisition, your data strategy should prioritize customer analytics capabilities. If operational efficiency is paramount, focus on process optimization and predictive maintenance applications.

Integrate with AI Strategy

Modern data strategy must also align with your organization's artificial intelligence initiatives. AI systems require high-quality, accessible, and well-structured data to function effectively. Your data strategy should anticipate AI use cases and ensure

that data collection, storage, and processing capabilities can support both current and planned AI applications.

This integration is bidirectional; your AI strategy will inform data requirements, while your data capabilities will constrain or enable AI possibilities. Organizations that treat these as separate initiatives often find themselves with incompatible systems and missed opportunities.

Establish Core Components

Data Quality Management: Implement systematic approaches to ensure data accuracy, completeness, consistency, and timeliness. Poor data quality undermines all downstream applications and decision-making processes. Establish clear quality metrics and monitoring procedures.

Data Architecture and Infrastructure: Design scalable systems that can accommodate current needs while supporting future growth. Consider cloud platforms, data lakes, warehouses, and integration tools that align with your technical requirements and budget constraints.

Compliance and Regulatory Adherence: Address industry-specific regulations such as GDPR, HIPAA, SOX, or financial services requirements. Build compliance considerations into data collection, storage, and processing workflows from the beginning rather than as an afterthought.

Data Analytics and Business Intelligence: Develop capabilities for descriptive, diagnostic, predictive, and prescriptive analytics that align with business needs.

Ensure that insights can be effectively communicated to decision-makers through appropriate visualization and reporting tools.

Data Security and Privacy: Implement robust security measures including access controls, encryption, and monitoring. Privacy by design should be embedded throughout your data lifecycle management processes.

Resource Planning and Investment: Allocate sufficient budget and personnel for both initial implementation and ongoing operations. Data strategy requires sustained investment in technology infrastructure, software licenses, and human capital. Plan for multi-year budget commitments that account for scaling requirements and technology evolution.

Long-Term Training and Capability Development: Establish comprehensive training programs for technical teams, business users, and leadership. Data literacy across the organization is essential for strategy success. This includes ongoing education in new tools, methodologies, and regulatory requirements. Consider partnerships with educational institutions and professional development programs to build internal expertise systematically.

Strategic Roadmap Development: While not explicitly required, developing a clear roadmap often helps ground both strategy design and consumption participants in terms of the objectives they are trying to achieve and what they need to design for. A well-constructed roadmap provides temporal context for initiatives, dependencies between components, and milestone definitions that enable effective progress tracking and stakeholder communication. This roadmap must integrate training schedules, budget allocation timelines, and resource acquisition plans, ensuring all components remain in alignment with each other and with the

driving organizational and AI strategies. These strategies will have specific temporal expectations for when capabilities, personnel, and infrastructure need to be operational.

Design Data Governance Last

Data governance represents the policies, procedures, and organizational structures that ensure data is managed as a strategic asset. This component comes last in your planning process because governance frameworks must be built around what you are actually governing.

Your data governance program should be driven by both organizational strategy and AI strategy requirements. It encompasses data stewardship roles, decision rights, quality standards, and compliance procedures. Without understanding your data landscape, strategic objectives, and AI requirements, governance becomes an abstract exercise rather than a practical management tool.

Effective governance includes clear accountability structures, standardized processes for data management, and mechanisms for continuous improvement. Key components typically include:

Data ownership and stewardship roles: Clear assignment of responsibilities for data quality, access decisions, and lifecycle management with appropriate training programs to ensure owners and stewards understand their duties, technical requirements, and regulatory obligations

Data classification and cataloging: Rather than attempting to catalog everything (an approach where most efforts fail horribly), consider a more thoughtful

approach that identifies a small and clearly defined set of critical data elements and computations. Each identified asset should have clean definitions, practical examples, and designated ownership to ensure successful implementation and ongoing maintenance

Access controls and security policies: Role-based permissions, data sharing protocols, and breach response procedures

Quality monitoring and remediation: Ongoing measurement of data quality metrics with defined processes for addressing deficiencies

Compliance and audit frameworks: Regular assessment of regulatory adherence with documentation and reporting capabilities

Change management processes: Controlled procedures for data schema modifications, system updates, and policy changes

A Data governance committee: A cross-functional decision-making body responsible for non-trivial data decisions that affect the entire organization rather than individual departments, setting enterprise-wide standards, arbitrating disagreements between stakeholders, and ensuring that governance frameworks are functioning effectively and strategy execution remains on track

Governance should enable rather than hinder data strategy and utilization while maintaining appropriate controls.

Implementation

Successful data strategy implementation requires executive sponsorship, cross-functional collaboration, and incremental delivery. Start with high-impact use cases that demonstrate value quickly, then expand systematically. Invest in change management and user training to ensure adoption.

Monitor progress against defined metrics and be prepared to adjust your approach based on lessons learned and changing business requirements. Data strategy is not a one-time planning exercise but an ongoing capability that must evolve with your organization.

Next Steps

Building a comprehensive data strategy requires careful consideration of organizational context, strategic objectives, and technical capabilities. By aligning data initiatives with business strategy and AI goals, establishing robust core components, and implementing thoughtful governance, organizations can transform data from a compliance burden into a competitive advantage.

The key is to approach data strategy as an integrated business capability rather than a technical project, ensuring that investments in data infrastructure and capabilities directly support organizational success.

How to Build a Data Strategy Part II: Insurance Company Considerations

Building on the foundational data strategy principles outlined in Part I, above, insurance companies face unique challenges and opportunities that require specialized approaches. The insurance industry operates within a complex regulatory environment while managing diverse data types from underwriting and claims to catastrophe modeling and customer interactions.

Insurance-Specific Strategic Alignment

Insurance companies must align their data strategy with both business objectives and regulatory mandates. Unlike other industries, insurance operates under state-by-state regulatory frameworks, federal oversight, and international requirements for global carriers. Your data strategy must support traditional functions like underwriting, claims processing, and actuarial modeling while enabling emerging capabilities in predictive analytics, fraud detection, and customer experience optimization.

Consider how data can enhance core insurance functions: improving risk assessment accuracy, reducing claims processing time, detecting fraudulent activity, optimizing pricing models, and enhancing customer retention. These capabilities directly impact profitability, regulatory compliance, and competitive positioning.

Regulatory and Compliance Foundations

Insurance data strategy must address multiple regulatory layers including state insurance commissions, NAIC requirements, federal regulations like Gramm-Leach-Bliley Act, and emerging privacy laws such as CCPA and state privacy legislation. International operations add GDPR and other regional requirements.

Rate filing processes require transparent, auditable data lineage from source systems through actuarial models to filed rates. Solvency monitoring demands real-time access to financial and operational data. Claims handling must comply with unfair claims practices regulations while maintaining detailed audit trails.

Build compliance requirements into your data architecture from the beginning rather than retrofitting systems later. This includes data retention policies that balance regulatory requirements with storage costs, and access controls that satisfy both business needs and regulatory expectations.

Core Insurance Data Strategy Components

Data Quality Management: Insurance requires exceptionally high data quality standards given regulatory scrutiny and financial impact of decisions. Implement systematic approaches ensuring accuracy, completeness, and consistency across underwriting data, claims information, and financial reporting. Poor data quality can result in regulatory sanctions, incorrect reserves, and flawed pricing models. Establish quality metrics specific to insurance operations including policy data validation, claims adjudication accuracy, and actuarial model inputs.

Data Architecture and Infrastructure: Design systems that accommodate both legacy mainframe operations and modern analytics platforms. Insurance companies typically operate significant legacy mainframe and AS/400 systems containing decades of critical business data. Your data strategy must address modernization without disrupting core operations or losing historical information essential for trend analysis and regulatory reporting.

Consider hybrid approaches that maintain core processing on proven platforms while creating modern data lakes for analytics and new applications. API strategies can bridge legacy systems with cloud-based analytics platforms. Plan for gradual migration pathways that minimize operational risk while enabling new capabilities.

Data extraction from legacy systems often requires specialized skills and careful planning to maintain data integrity. Plan for data volumes that spike during catastrophic events and seasonal business cycles.

Regulatory Compliance and Adherence: Beyond general privacy regulations, address insurance-specific requirements including state insurance codes, NAIC reporting standards, Gramm-Leach-Bliley Act, and fair lending practices. Build audit trails that satisfy regulatory examinations and support rate filing processes. Implement data retention policies that balance regulatory requirements with operational efficiency and storage costs.

Insurance Analytics and Business Intelligence: Develop capabilities supporting actuarial modeling, underwriting decisioning, claims analytics, and financial reporting. This includes loss development analysis, catastrophe exposure management, fraud detection algorithms, and customer lifetime value modeling.

Ensure analytics platforms can handle insurance-specific calculations including reserves, risk-based capital, and solvency monitoring.

Insurance companies must integrate catastrophe modeling data from vendors like RMS, AIR, and CoreLogic with internal exposure data, requiring sophisticated data management capabilities that can process large-scale simulations, geographic information systems, and real-time exposure tracking.

Your data architecture must support scenario analysis, stress testing, and regulatory reporting for natural disasters, cyber events, and other emerging risks. Plan for data storage and processing capabilities that can handle periodic intensive modeling while maintaining cost efficiency during normal operations.

Data Security and Privacy: Implement robust security measures protecting sensitive policyholder information, financial data, and proprietary underwriting models. Address both external threats and insider risks common in insurance operations. Privacy controls must accommodate customer service needs, claims investigation requirements, and regulatory examination access while protecting personal information.

Resource Planning and Investment: Allocate resources for both maintaining legacy systems and developing new capabilities. Insurance data strategy requires sustained investment in actuarial talent, data science capabilities, and specialized insurance technology. Plan for regulatory compliance costs and vendor management relationships essential to insurance operations.

Long-Term Training and Capability Development: Build insurance-specific data literacy across underwriting, claims, actuarial, and finance teams. This includes

training on regulatory requirements, industry-standard models, and emerging technologies like telematics and predictive analytics. Develop partnerships with actuarial organizations and insurance technology vendors for ongoing education.

Strategic Roadmap Development: Create roadmaps that integrate regulatory filing schedules, business planning cycles, and technology refresh requirements. Insurance roadmaps must align with annual statement preparation, rate filing deadlines, and regulatory examination schedules. Include catastrophe modeling updates, system modernization projects, and compliance initiative timelines while ensuring all components remain synchronized with organizational strategy and emerging AI capabilities.

Implementation for Insurance

Insurance data strategy implementation requires particular attention to regulatory approval processes, actuarial validation, and business continuity. Start with use cases that demonstrate clear business value while building confidence in data quality and governance procedures.

Regulatory bodies often require advance notification of significant system changes. Include regulatory communication in your implementation timeline. Actuarial teams must validate that new data sources and models produce reasonable results compared to historical experience.

Plan implementation in phases that maintain operational capabilities while building new functions. Insurance operations cannot tolerate data outages during critical periods like catastrophe events or regulatory reporting deadlines.

Specialized Governance Considerations

Insurance data governance must address unique industry requirements including actuarial independence, regulatory examination readiness, and cross-functional data sharing between underwriting, claims, and finance organizations.

Establish clear protocols for model validation, assumption changes, and data source modifications that could impact financial results. *Include actuarial review in your data governance committee structure.* Document data lineage requirements that satisfy both internal audit and regulatory examination standards.

Address data sharing agreements with reinsurers, vendors, and industry organizations while maintaining competitive confidentiality and customer privacy. Insurance companies often participate in industry data sharing initiatives that require careful governance frameworks.

Next Steps

Building an effective data strategy for insurance companies requires balancing traditional industry practices with modern capabilities. Success depends on understanding regulatory requirements, legacy system constraints, and unique business processes while implementing governance frameworks that enable innovation within appropriate risk parameters.

Insurance companies that thoughtfully address these industry-specific considerations while following core data strategy principles will be positioned to

improve operational efficiency, enhance risk assessment capabilities, and deliver superior customer experiences in an increasingly competitive market.