A CEO's Strategic Guide to AI

Stepping Into the AI Age

LIMRA LOMA

Navigate With Confidence

A CEO's Strategic Guide to AI

Stepping Into the AI Age

For Additional Information:

Kartik Sakthivel, Ph.D., MS-IT/MS-CS, MBA, PGC-IQ
Vice President & Chief Information Officer
LIMRA and LOMA
ksakthivel@limra.com

Created in collaboration with the LIMRA and LOMA AI Governance Group

Contents

Figures

1.0 Executive Overview

The financial services sector is undergoing a dramatic and transformative evolution driven by advancements in artificial intelligence (AI) and generative AI (GenAI) as a derivative of the overall AI industry. The introduction of AI across the value chain is not just enhancing existing processes, but it is also fundamentally reshaping the life insurance landscape. By capitalizing on AI — correctly — insurers can achieve significant competitive advantages, drive innovation, and better serve a new generation of customers in a digital world.

The continuously accelerating pace of AI evolution presents unlimited potential to transform the insurance industry and society as a whole. However, these rapid advancements can also usher in a new set of risk management challenges. As the industry continues its mission to financially protect underserved communities and deliver affordable protection to the uninsured and underinsured, missteps in AI implementations can have far-reaching implications.

Small to midsize carriers encounter a distinct operational challenge. They must balance the imperative to modernize and stay competitive with resource constraints — while updating processes and systems, enhancing workforce skills, and managing increasing dependence on third-party vendors. AI provides a strategic solution, not via large-scale transformation initiatives, but by selectively deploying intelligent AI approaches to address critical issues, streamline routine tasks, and enable teams to perform more effectively and efficiently.

According to the 2025 Insurance Barometer Study from LIMRA and Life Happens, nearly 100 million Americans are uninsured or underinsured. This playbook is intended to serve as a guide for C-suite leaders of small to midsize carriers, which play a critical role in helping to close this protection gap. It provides a high-level, step-by-step roadmap that is tailored for small to midsize carriers to responsibly adopt AI.

Taking a pragmatic approach, it is grounded in LIMRA insights, lessons derived from the LIMRA and LOMA AI Governance Group (AIGG), and engagement with executives across the industry. It is based on practical considerations, business value, and regulatory compliance. This playbook intends to enable companies to implement solutions without requiring extensive AI modeling teams, software engineering teams, data teams, or a significant investment in infrastructure — and without exposure to unnecessary risks. By following its repeatable and adaptable framework, leadership can realize the advantages of AI, while maintaining sound oversight and governance practices. Employing the LIMRA and LOMA AIGG tools, scorecards, frameworks, best practices, and industry standards will provide a process that progressively assuages employee concerns around AI, while enhancing internal expertise and confidence.

2.0 Guiding Tenets

The use of AI within our industry can no longer be viewed as an abstract future trend. Instead, AI already is ubiquitous, and this ubiquity has been achieved at lightning speed — with an explosive growth unlike any other technology before it. AI is already embedded in the tools, platforms, and customer expectations that shape the insurance industry. For small to midsize life insurance carriers, AI represents both a competitive opportunity and a manageable risk. But unlike large insurers with deep technical teams and innovation labs, they must chart a different course.

This playbook is designed for small to midsize carriers, recognizing that smaller carriers need to do more with less; manage expense pressures while focusing on sustainable growth; operate with lean internal teams; rely on third-party platforms, off-the-shelf solutions, and vendors for core operating functions; and tightly manage regulatory, reputational, and operational risks. All the while, they must measure and demonstrate value from AI, seeking to stay competitive in the market segment and against larger carriers.

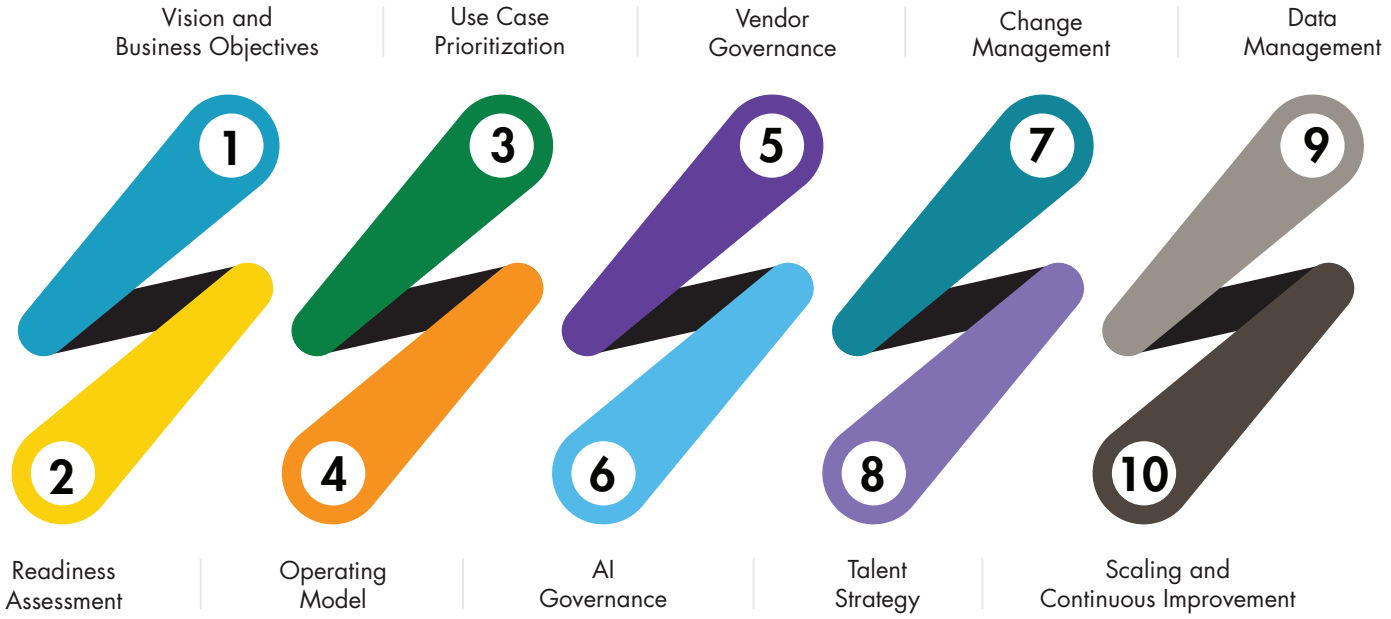
With that in mind, instead of taking a "build" approach, this playbook focuses on a "buy" or "partner" approach to AI. Small to midsize firms have an opportunity to realize success by leveraging AI already available in the vendor ecosystem; focusing on low-risk, high-value use cases; adopting LIMRA and LOMA AIGG resources; establishing basic governance to maintain transparency and compliance; starting small and scaling slowly; measuring business value generated; and upskilling employees to capitalize on available AI tools. This is not an AI strategy or a technology strategy — but rather a business modernization playbook that happens to use AI as the strategic lever.

3.0 AI Playbook Framework

This AI playbook is based on 10 major, interrelated steps (Figure 1). These steps are generally sequential in nature, and they need to be conducted in their respective positions. However, there are some notable steps — such as Vendor Governance, AI Governance, and Change Management — that are developed and executed on an ongoing basis, meaning they can be planned and executed in parallel. (Note: There are LIMRA and LOMA AIGG tools, frameworks, best practices, and industry standards to assist with each step of this process.)

The next sections provide an overview of the 10-step playbook and expand on each step.

Figure 1 — The 10-Step AI Framework



3.1 PLAYBOOK FRAMEWORK – 10 STEPS

Step 1. Vision and Business Objectives
Define a clear vision for how AI will advance your organization's mission and outline measurable strategic objectives. This step centers on aligning AI initiatives with business priorities; ensuring leadership buy-in; and setting a guiding direction for innovation, competitiveness, and customer value. Ideally, AI implementations should be anchored to your organization's business priorities and strategic objectives (such as growth or operational efficiency).

Step 2. Readiness Assessment
Evaluate your organization's current capabilities, maturity, infrastructure, and cultural preparedness for AI adoption. This includes identifying skill gaps, technology constraints, and strengths or weaknesses to inform the path forward.

Step 3. Use Case Prioritization
Resist the urge to launch multiple AI pilots, which may dilute your focus. Start small, establish early wins, learn from the pilots, and then scale. Identify, categorize, and prioritize AI use cases that offer the highest business value with manageable risk. Focus on applications where AI can streamline operations and deliver measurable return on investment.

Step 4. Operating Model
Adopt an "AI as a Service" approach by partnering with reputable third-party vendors — including some of your current partners. This means leveraging off-the-shelf AI solutions and platforms, rather than building in-house, which should accelerate deployment, control costs, and access advanced capabilities without the need for specialized internal teams.

Step 5. Vendor Governance
Establish robust oversight of third-party AI vendors to ensure compliance, data security, performance monitoring, and alignment with your business goals. Regularly review and update contracts, performance metrics, and service delivery to mitigate operational and reputational risks.

Step 6. AI Governance
Implement a framework for the ethical, transparent, and responsible use of AI. This involves setting policies for risk management, regulatory compliance, data privacy, and ongoing model monitoring — ensuring AI is used safely and in a way that builds trust with stakeholders. Regulators in multiple states are asking carriers to have such a structure in place.

Step 7. Change Management
Prepare your organization for AI-driven transformation by communicating the vision, addressing employee concerns, and fostering a culture of adaptability. This includes training, stakeholder engagement, and support structures to promote adoption, minimize resistance, and maximize chances of success with your AI implementations.

Step 8. Talent Strategy
Develop and execute plans to educate and upskill existing staff and attract new talent capable of working with AI tools and solutions. AI literacy should be a key part of your firm's AI playbook. The emphasis should be on practical knowledge and the ability to leverage AI in day-to-day operations, even without the need for technical expertise.

Step 9. Data Management
Build a foundation of high-quality, secure, and well-governed data to support AI initiatives. This step covers data acquisition, integration, cleansing, privacy, and stewardship, ensuring reliable and compliant inputs for AI models and solutions.

Step 10. Scaling and Continuous Improvement
After initial pilots, expand successful AI applications across your firm, while fostering an environment of ongoing learning and adaptation. Continuously measure impact, refine use cases, and incorporate feedback to drive sustainable value and keep pace with evolving AI technologies.

3.2 PLAYBOOK FRAMEWORK – 10 STEPS EXPLAINED

3.2.1 Step 1. Vision and Business Objectives

This step ensures that AI does not "exist in a vacuum." In other words, it is crucial to ensure that AI is not a technology for technology's sake. Stakeholders must be able to establish a clear correlation between your strategic goals and business objectives and AI as an enabling technology. It is important for C-suite leaders to anchor AI to business value with clear, reasonable ambitions tied to operational excellence, process efficiency, and customer experience.

It is not necessary for your organization to establish AI as a competitive differentiator. You do not need to "compete on AI" — at least not yet, anyway — but you currently do need to use AI to compete smarter. As you anchor AI as an enabling technology to advance business objectives, consider starting with strategic goals that promote operational efficiency. For

instance, you can establish a corporate objective to leverage AI responsibly and efficiently to reduce manual workloads, enhance decision-making, and improve customer and agent experiences — balanced with respecting budgetary, ethical, and regulatory boundaries.

Once you have clearly anchored AI as enabling strategic business objectives, you will create AI-as-an-enabler goals predicated on your business goals. Business goals aligned to their AI enablers include:

a. **Business Goal (Operational Efficiency):** Reduce operating expenses by x percent in n years. **AI Enablers:** Task automation, document handling.

b. **Business Goal (Agent Satisfaction):** Improve agent satisfaction by y percent. **AI Enablers:** AI-driven agent support, faster AI-powered quoting tools.

c. **Business Goal (Customer Satisfaction):** Improve Net Promoter Score (NPS) by z percent. **AI Enabler:** AI-powered chatbots.

d. **Business Goal (Customer Satisfaction, Agent Satisfaction, and Operational Efficiency):** Accelerate quote-to-bind by n percent. **AI Enabler:** AI-powered document ingestion and form pre-fill.

As your firm aligns business goals with AI as an enabling technology, there are three overarching principles to keep in mind as your guide:

1. **Prioritize Pragmatism Over Perfection:** Focus on low-effect and high-yield use cases. Beware of becoming entrapped by the pursuit of perfection and "analysis paralysis." AI is moving so quickly that things will never be just right or perfect.

2. **To Begin, Begin:** It is more important to begin and assume the risk that the results might be incongruent with expectations. Starting small will allow for controlled implementations and a faster time to market. If a use case falls short of expectations, smaller use cases are more palatable to miss the mark than are larger or broader ones.

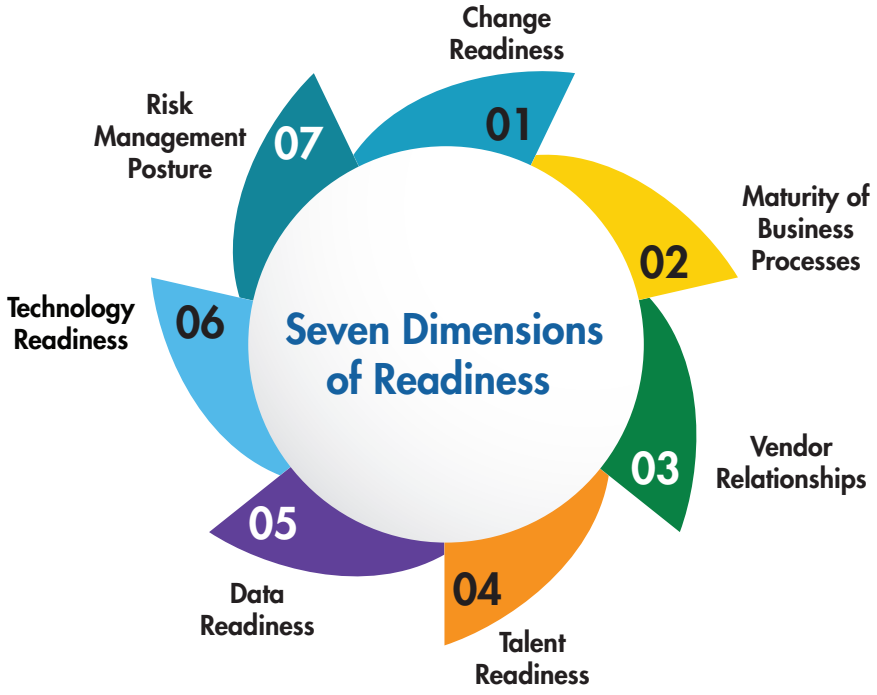
3. **Rely on Third-Party Vendors — With Intent and Intelligence:** Lean on your existing third-party vendors and SaaS providers. However, ensure that you maintain governance and oversight, since these factors are especially important with respect to AI. Clearly document AI transparency needs with your vendors via contracts and ensure that these are regularly updated. Derisking the vendor supply chain is vital. For instance, whereas your primary AI service provider might conform to your governance requirements, it may rely on a number of other AI providers for services — and these providers might not have the same rigor as your direct vendor. Rely on your ecosystem partners, but ensure that you have a clear line of sight into "daisy chain" vendors, and establish accountability and responsibility early on.

3.2.2 Step 2. Readiness Assessment

The success of any AI initiative begins not with technology, but with a candid evaluation of your organization's readiness for leveraging AI. Performing a comprehensive readiness assessment is not just a "check off the box" exercise. It should be treated as a strategic imperative that will guide your approach, future investments related to scaling AI, and implementation timelines. By conducting a readiness assessment with clear, actionable steps, firms can ensure they are equipped not just to "give AI a shot," but to adopt it in a business-aligned, responsible, ethical, compliant, and repeatable way. Most of all, a readiness assessment will provide the basis to determine how much business value is generated by leveraging AI within certain parts of the company.

Firms are encouraged to revisit this assessment periodically — and certainly before embarking on any new broad AI initiatives. Its goal is to help transform a static checklist into a living, breathing strategy that evolves with your firm's needs and delivers meaningful, measurable business value. It will help you understand where you are and what you need before launching AI initiatives by assessing organizational, technical, and operational readiness for AI adoption. Also, it will help you identify minimal viable investments for AI success — without overwhelming budgets or resource capacity. Figure 2 illustrates the seven primary dimensions of readiness assessment. Note that the numerical order in which these dimensions are listed does not imply order of importance. That being said, dimensions 1 and 2 — Change Readiness and Maturity of Business Processes — are where you would logically start evaluating your AI journey.

Figure 2 — Seven Dimensions of Readiness Assessment



Assessment Dimensions

Dimension	Why	Assess
Change Readiness	Understand how AI will be received, adopted, and utilized by your workforce. If your organization is resistant to change — especially regarding how they conduct their tasks and business processes — change management will be of paramount importance. The greater the change management required, the more reason to start small, test and learn, and then scale.	You will need to understand historically how new tools and technology have been received by your workforce and what kind of change management principles were needed at the time. You should be able to assess the culture of your organization via leadership, a staff survey, and/or a focus group of employees. Next, you can identify champions and skeptics. Ideally, you should implement AI *with your employees*, rather than *impose it upon them*. From there, develop a communication plan for AI initiatives, emphasizing benefits and addressing concerns with transparency. Assuage employee concerns about AI — ensuring they understand it is intended to augment their jobs and not to replace them. Focus on potential productivity gains in the context of where this time and energy can be redeployed, and avoid using language that employees can misinterpret as job action.
Maturity of Business Processes	Successful AI implementation will require your firm to rethink, reimagine, and reinvent your existing business processes. AI cannot exist as a standalone technology, and you should not automate a problematic business process. AI implementations work best with predictable, rote, repeatable, and operational processes.	Determine the maturity of your business processes for AI adoption by reviewing the repeatability, consistency, and predictability of process outcomes and outputs. Ensure that processes are documented and not resident within one individual employee.
Vendor Relationships	It is likely that small to midsize firms will use AI services through existing vendors and software providers. Your success implementing AI will implicitly be determined by the strength of these relationships in terms of governance, transparency, and AI oversight. It is imperative to ensure that contract language reflects vendors incorporating AI into their standard product offerings. In addition, several vendors offer AI-enhanced capabilities at an additional cost as add-on services. Therefore, it is important to capitalize on the strength and size of existing engagements to procure AI capabilities at a reasonable price.	Conduct an evaluation of the vendor product roadmap. Many vendors already have incorporated AI within their existing base products. Other AI services are available for "free" to most companies as a part of their existing enterprise licensing. For example, Microsoft Copilot with Enterprise Data Protection is a private Large Language Model/GPT that allows your firm's data to stay private, that is, not to be used to train public AI. This mitigates risk of accidental loss of intellectual property, company private data, or proprietary data to a public AI system. Copilot with Enterprise Data Protection offers standard capabilities such as chat, brainstorming, document summarization, and authoring drafts. Start simply by listing all vendors and third-party tools. Request product roadmaps to understand their AI capabilities and future direction. If gaps are found, explore new vendor relationships or pilot programs with providers offering AI-enabled solutions.

Assessment Dimensions (continued)

Dimension	Why	Assess
Talent Readiness	For your organization, success with AI might not require a full team. However, it will require a team that is ready, willing, capable, educated, and literate on how to leverage the tools you are providing them. The promise of AI's potential can only be realized with a workforce that is engaged and leans into adoption.	Evaluate your workforce for change champions and advocates who could be early adopters of AI, as well as "ambassadors" of its use across their teams. In addition, assess which employees best understand your business. They will be best equipped to identify the key considerations involved when overhauling or reimagining your existing business processes. Leadership support will be another critical factor — especially when it pertains to changing business processes across the value chain. Prioritize educating your teams with domain knowledge that provides business context when they apply AI, as well as with basic AI literacy. This will increase their effectiveness in using these tools. Finally, inventory current staff capabilities and external resources (such as consultants, advisors, and fractional AI leadership) you can turn to for expertise. Identify at least one internal or external resource with AI literacy, and invest in basic AI education for leadership.
Data Readiness	AI is only as good as the data it is provided. It is impossible to have great AI with bad data. Historically, our industry has not treated data as an asset. Data management and governance — which includes quality, availability, accuracy, privacy, security, accessibility, and governance —is going to be vital. This is especially true of traditional AI, such as with automated and accelerated underwriting. In this case, you would provide your applicant information, proprietary data, and bespoke underwriting rules to an external third-party vendor, and the vendor would provide an output or a deterministic result.	Consider commissioning data audits related to the AI use case to identify sources, gaps, and silos. Document the structured data (such as databases and spreadsheets) and unstructured data (such as emails and PDFs) that you possess. If gaps exist, prioritize addressing them before providing that data to AI. Establish basic data governance standards by appointing data stewards, and set protocols for data entry, access, and regular quality checks.
Technology Readiness	Every carrier has specialized systems, such as policy administration systems (PAS) and claims systems. Every carrier also has standard enterprise software, such as the Microsoft Office suite and SharePoint. Unfortunately, most carriers also have legacy systems with workarounds that have been institutionalized as business processes around them. These are notoriously challenging to uncoil. These systems also house a significant amount of enterprise institutional knowledge in terms of data. Your AI systems should alleviate your problems, not create new ones. In simple terms, AI systems should be easily integrated into the range of tools and platforms you currently leverage. This assessment is important to determine how well AI can integrate with existing systems — including core systems like PAS, claims, customer relationship management (CRM), and cloud. The AI solution should also be aligned with your existing cybersecurity posture.	To conduct a technology assessment, consider going beyond conducting an inventory of your systems. Instead, focus on mapping how they communicate (or fail to communicate) with a proposed AI system. If the AI product is a "lay up," then it should be considered an easier solution to integrate. This is why existing vendor relationships are so important. As the vendors integrate AI into their base products, as long as you have relied on the "configure and not customize" approach, you should be able to tap into these AI capabilities. Review vendor contracts for flexibility and support for AI features. When conducting this technology assessment, consider both on-premise and cloud tools, as well as third-party integrations.

Assessment Dimensions (continued)

Dimension	Why	Assess
Risk Management Posture	This prevents inadvertent compliance issues or public perception risks. Ensure that you pay special attention to the new cybersecurity landscape, as well as data privacy and protection state-based regulations.	Review the LIMRA and LOMA AIGG papers on the NIST standards, the NAIC Model Bulletin, and Governance Best Practices. Stay informed of AI-related regulations (NAIC and state), and continuously reevaluate your internal risk appetite. Identify which regulations apply to your organization and determine whether you have policies in place to address AI-specific risks, such as explainability, bias, and consumer protection. Establish a regular schedule (quarterly or biannual) for reviewing AI-related compliance risks and updating policies accordingly.

Readiness Assessment Framework

Carriers can use the framework template below, referring to the scoring guide and rubric. You are encouraged to edit it (by adding and/or removing items) to ensure it fits your needs and your firm's requirements. If edits are made, ensure the scoring criteria are adjusted appropriately. This framework represents a starting point that can be applied as is; however, firms should make adjustments as needed.

Dimension	Assessment Questionnaire	Points
Change Readiness	• Has our company successfully adopted a new system or tool in the last two years? • Do leaders support responsible use of new technology like AI? • Is there a culture of learning and adaptability within our workforce? • Do we communicate technology changes clearly and early? • Do we have any change champions or early adopters on staff?	For each question, score as follows: • Yes = 2 points • Partial / In Progress = 1 point • No = 0 points
Maturity of Business Processes	• Are core business processes (such as underwriting, claims, and servicing) well-documented? • Are these processes followed consistently across teams? • Do the processes contain steps that are highly manual and repetitive? • Are there existing process owners or subject matter experts for each workflow? • Have we already automated or optimized parts of the workflow?	For each question, score as follows: • Yes = 2 points • Partial / In Progress = 1 point • No = 0 points
Vendor Relationships	• Do we know which vendors already use AI within their solutions? • Do our vendor contracts allow for audit, transparency, or oversight? • Do we meet with vendors at least quarterly to discuss product capabilities? • Do we have strong IT or consultant support to help evaluate new technology options? • Are we comfortable relying on vendors to co-manage AI features or pilots?	For each question, score as follows: • Yes = 2 points • Partial / In Progress = 1 point • No = 0 points

Readiness Assessment Framework (continued)

Dimension	Assessment Questionnaire	Points
Talent Readiness	• Do we have at least one person with experience in data, automation, or digital tools? • Can we designate someone (even part-time) to coordinate AI exploration? • Are we open to hiring a consultant or vendor partner for AI planning? • Do we offer or support GenAI or automation learning (formally or informally)? • Does our IT team have capacity to participate in a pilot project?	For each question, score as follows: • Yes = 2 points • Partial / In Progress = 1 point • No = 0 points
Data Readiness	• Do we consistently capture structured data (such as policies, claims, and underwriting notes)? • Is our data clean and mostly free from duplication or formatting errors? • Do we have access to key data sources via export or reporting tools? • Is our unstructured data (such as PDFs, emails, and call notes) tagged or searchable? • Do we have any data standards or guidelines (even informal ones) in place?	For each question, score as follows: • Yes = 2 points • Partial / In Progress = 1 point • No = 0 points
Technology Readiness	• Do we use modern systems (such as PAS, Claims, and CRM) that support data export or integration? • Do any vendors offer embedded AI tools or smart features? • Is our infrastructure cloud-based or hybrid, supporting external integrations? • Do we use any no-code/low-code platforms internally? • Can we launch trials of external tools or SaaS with minimal disruption or IT burden?	For each question, score as follows: • Yes = 2 points • Partial / In Progress = 1 point • No = 0 points
Risk Management Posture	• Do we understand AI-related regulations (including NAIC, state Departments of Insurance (DOIs), and privacy laws)? • Do we involve compliance or legal before adopting any AI-related technology? • Do we require vendors to disclose use of AI or algorithms? • Do we maintain audit logs or document automated decisions? • Do we have a defined process to respond to AI-related issues?	For each question, score as follows: • Yes = 2 points • Partial / In Progress = 1 point • No = 0 points

Scoring Instructions

Add up your score per dimension to identify High, Moderate, or Low Readiness. Most small carriers will find themselves between Low to Moderate Readiness. The goal is not to "catch up" overnight, but to align your strategy with your current situation. This will build foundational capabilities that set the stage for responsible, incremental AI adoption.

Rubric (Per Dimension)

8 to 10 points: High Readiness — Proceed with AI planning and pilot use cases.

4 to 7 points: Moderate Readiness — Proceed with caution and address key gaps.

0 to 3 points: Low Readiness — Focus on foundational improvements and launch internal GenAI tools, such as Copilot.

3.2.3 Step 3. Use Case Prioritization

To develop a sustainable and effective AI strategy, it is essential for C-suite leaders to prioritize AI use cases intentionally and systematically. The goal is not to rush into AI adoption, but to align initiatives with your current level of readiness and organizational capacity — creating a scalable roadmap for responsible innovation.

Only by modeling value in realistic, incremental terms will your firm be able to identify the most viable AI use cases based on business impact, implementation feasibility, and cost efficiency. Before beginning a prioritization exercise, leaders should clarify the business challenges and/or opportunities AI could address within your firm.

Common objectives might include:

- Automating manually intensive processes
- Reducing manual processing time for policy applications
- Improving customer service responsiveness
- Enhancing accuracy in underwriting decisions
- Mitigating operational risks and errors

When prioritizing use cases, it is very important to ensure the underlying business processes are robust enough — well-defined, repeatable, documented, and optimized — for AI to support their automation. You do not want to automate a problematic process. Successful AI implementation should cause you to evaluate current means of working and whether these are appropriate for the future. It also will be vital for leaders to engage key stakeholders across the value chain, from IT and legal to compliance and customer experience. This will ensure that prioritized use cases align with divisional and departmental goals, as well as enterprise objectives.

Table 1 depicts a simple, standard prioritization grid.

Table 1 — 2x2 Prioritization Grid

Feasibility ▶ / Impact ▼	HIGH	LOW
HIGH	Start Here	Monitor for the Future
LOW	Evaluate With Caution	Avoid / Do Not Pursue

This approach provides clarity and ensures resources are directed toward initiatives with the greatest strategic business value. Table 2 provides a guide on how to use it in prioritization efforts.

Table 2 — Prioritization Guide

Feasibility ▶ / Impact ▼	HIGH	LOW
HIGH	Prioritize pilot projects in this quadrant. These are likely quick wins that can generate momentum and demonstrate value early.	Track advancements and revisit as internal capabilities grow or external solutions mature.
LOW	Consider only if resources are abundant or for compliance reasons.	De-prioritize these use cases to conserve effort and capital.

When evaluating each proposed use case based on feasibility and impact, you should create a weighted scoring matrix to rank them objectively. (For example, one to five points would be assigned for each criterion.) Prioritize those with the highest combined scores.

Scoring Criteria

Factors to Consider for Feasibility:

- Availability and Quality of Data
- Complexity of Integration Into Ecosystem (Process and Technology)
- Available Vendors and Third-Party Software Providers
- Internal Capabilities

Factors to Consider for Impact:

- Cost Savings and Operational Efficiencies
- Improvements to Customer Experience
- Risk Reduction
- Improvements in Time to Market

Next, build an inventory of your AI use case pipeline. For the use cases that rank the highest, lead your executive team to map out actionable steps with clear milestones. These actionable steps include:

- Define measurable success criteria. (For example: reduce processing time by n percent, boost accuracy rate targets by x percent, and improve customer satisfaction metrics as measured by an NPS score increase from a to b)
- Identify quick-win pilots that can be implemented within three to six months and have tangible benefits.
- Establish a feedback loop with pilot users to iterate and refine the solution.
- Develop a knowledge repository to capture lessons learned and share best practices across the organization.

Also, institute quarterly or biannual reviews of the use case pipeline:

- Assess progress against defined milestones and key performance indicators.
- Assess, recalibrate, grade, and reprioritize use cases based on changes in internal readiness, market conditions, or AI advancements.
- Adopt a product development lifecycle, and be intentional about scaling, retiring, or pivoting use cases based on outcomes and feedback. You do not want to create an abundance of abandoned use cases within your portfolio.
- Be a visible and vocal champion to inspire and institutionalize a culture of experimentation and learning, rather than perfection. Allocate resources for small-scale pilots, ensure robust documentation, and celebrate incremental wins. By making use case prioritization a repeatable, data-driven process, you lay the groundwork for responsible and scalable AI adoption that is tailored to your organization.

The following examples of AI use cases may provide some guidance.

Sample High-ROI, Low-Complexity AI Use Cases

Use Case	Business Value	Impact	Feasibility
AI Document Intake and Automated Classification	Automate intake of life application submissions, forms, and medical records using Optical Character Recognition (OCR) and Natural Language Processing (NLP) capabilities	High (speed and accuracy)	High (many vendor tools available)
Automated Email Routing	Automated AI triage for agent and customer emails, routing them to the appropriate queue	Medium (operational efficiency)	High
Customer Service Chatbot	Reduce traffic from customer service agents, allowing an AI bot to handle FAQs on policy status, billing, claims, and address changes	High (call deflection)	Medium to High
Pre-Fill Underwriting Documents	Extract key values from APS and medical PDFs to pre-fill underwriting templates	High (manual effort reduction, quality increase due to reducing human errors)	Medium (vendor support)
AI Risk Flags in Underwriting	Pattern recognition to flag non-standard disclosures or age-inconsistent values	High (risk mitigation)	Medium
Call Transcription and Sentiment Analysis	Monitor sales or customer service calls for tone, quality, and potential issues	Medium	Medium
Fraud Detection	A derivative of the above, leveraging vendor AI tools to flag various kinds of insurance fraud	High	High
Content Personalization for Agents	Recommend email content or sales materials based on geography, product, or similar factors	Medium (agent productivity lift)	High (low-barrier GenAI)

Sample AI Use Cases to Revisit as Maturity Increases

Use Case	Need for Caution
Predictive Modeling for Mortality	To implement successfully, you require a high degree of data science maturity and actuarial alignment.
Full AI-Based Underwriting	This requires rigorous testing, high-quality data, focused attention to prevent bias, strong information and data privacy practices, robust cybersecurity, robust compliance and auditability, and strong technology and data infrastructure.
Generative AI for Legal Drafting	There is always a risk of hallucination with GenAI. Unless "human-in-the-loop" is an integral part of implementation, it is not yet reliable without strong human review.

Using CBA and Determining ROI

The LIMRA and LOMA AIGG has developed six cost-benefit analysis (CBA) templates and strategic guides, as well as a return on investment (ROI) calculator.[1] The CBA resources include:

[1] These resources are available on LIMRA.com and LOMA.org, and either a LIMRA.com or LOMA.org account is required to access these and other tools, frameworks, best practices, and industry standards. LIMRA.com site: Artificial Intelligence (AI) Tools and Resources and LOMA.org site: Artificial Intelligence (AI) Tools and Resources.

- **Traditional AI – Build In-House Strategic Guide:** A strategic guide on how to conduct a CBA for traditional AI built in-house
- **Traditional AI – Build In-House Turnkey Template:** A turnkey template for a CBA for traditional AI built in-house
- **Traditional AI – Third-Party Vendor Strategic Guide:** A strategic guide on how to conduct a CBA for AI procured from a vendor
- **Traditional AI – Third-Party Vendor Turnkey Template:** A turnkey template for a CBA for AI services procured from a vendor
- **Generative AI Strategic Guide:** A strategic guide on how to conduct a CBA for Generative AI
- **Generative AI Turnkey Template:** A turnkey template for a CBA for Generative AI

A downloadable calculator is also available, which serves as a turnkey way to calculate value dimensions and value drivers to derive AI ROI. It is strongly recommended that firms employ the appropriate CBA frameworks, with the most applicable likely to be the CBAs around third-party vendors and generative AI.

Note that full financial modeling is challenging for AI and might be especially difficult for small teams. With that in mind, the following are some parameters to consider as a "lite" version of an ROI framework.

Inputs

- Manual time to perform each task (minutes)
- Volume per month (for example, forms processed or emails routed)
- Average hourly rate of staff handling tasks
- AI automation rate (estimate from vendor or pilot)
- Software cost (monthly or per-seat)

Illustrative Example: AI Form Classification for New Life Policies

Metric	Value
Manual time spent per form	30 minutes
Forms per month	10,000
Staff hourly cost	$50
Automation potential	75%
Monthly software license	$10,000

Savings = (10,000 × 30 ÷ 60) x 50 x 0.75 = **$187,500/month saved**
Net ROI = $187,500 – $10,000 = **$177,500/month net benefit**

3.2.4 Step 4. Operating Model

The Operating Model section aims to equip the C-suite with a practical, repeatable framework for sourcing and integrating AI solutions. This guide empowers leaders to make informed choices about building, buying, or partnering for AI capabilities, ensuring maximum ROI and sustainable transformation. For small to midsize firms, the best sourcing approach for AI solutions is based on cost, talent access, speed to value, and vendor dependencies. Nearly all of the time, your firms will and should choose to buy or partner.[2]

AI Sourcing Options

In general, it is recommended for firms to default to "buy" and "partner" approaches for AI implementations, reserving "build" as more of a last choice for narrow, high-value needs.

Option	What It Means	Best When…
Build	Your firm would develop custom AI solutions in-house (such as machine learning models or chatbots). Your firm will construct AI solutions that are tailored to your company's unique needs. This path demands significant investment in technology, skilled teams (including data scientists and machine learning engineers), and ongoing maintenance. For most small to midsize carriers, this should be a "last resort" option, reserved for scenarios where proprietary data or processes provide a competitive edge — such as developing predictive models for niche products or automating specialized workflows. If you must build, initiate a discovery phase to map business needs against available internal talent. If internal capacity is limited, use no-code/low-code AI platforms to prototype solutions before committing resources. Leverage open-source models and stay focused on narrow, high-impact use cases. Finally, your firm might want to consider hiring fractional AI experts to fill gaps efficiently.	You have strong internal technology and data talent, or you have highly specific needs with a competitive or intellectual property advantage. This is the most resource-intensive option — in terms of cost and time. You will also be expected to entirely ensure your AI models are free of bias and establish a robust quality assurance and control program.
Buy	Your firm would purchase prebuilt AI features in existing software and/or purchase new AI utilities and tools. Most often, these will be turnkey in nature, but they might require some ecosystem integration depending on the use case. By purchasing ready-to-use AI functionality as part of existing software platforms, you will gain speed, lower upfront costs, and reliable vendor support. This is the easiest route, but your firm has to maintain an immutable "no customizations" policy. Do not allow yourself to bend the software to fit your processes; instead, adjust your processes and then overlay the AI. Start by conducting an inventory of your current SaaS tools to identify embedded AI features. Compare vendors for fit, transparency, and ease of integration within your technology ecosystem. Finally, update your vendor contracts to ensure that you always request demos, audit logs, and evidence of explainability and bias controls.	You need speed, cost efficiency, and out-of-the-box integration. For small to midsize carriers, this is the best option — primarily because by buying a vendor solution, you do not need to build out your own technology teams and infrastructure. Another major reason is that you will always benefit from platform advancements the vendor makes, as well as the steps it takes to protect the platform (from a cybersecurity perspective) and scale the product. This allows firms to focus on their core competency of running and growing their business.

[2] The LIMRA and LOMA AIGG has developed a paper and methodology to guide organizations in deciding whether to build, buy, or partner. This paper will be available on LIMRA.com and LOMA.org in the fourth quarter 2025. It is strongly recommended that C-suite leaders review it in addition to the abbreviated rationale presented here.

Option	What It Means	Best When…
Partner	Your firm would partner with vendors or consultants to develop or implement AI solutions. This provides the technical expertise and resources of these third parties, while they benefit from your business expertise. In collaborating with vendors, consultants, or system integrators to customize AI solutions, your firm will gain tailored capabilities without needing to invest in a homegrown effort and investing in full development resources. If you choose this option, structure your partnership agreements with clear deliverables, data protection policies, and ongoing support expectations. Establish regular checkpoints for review and adaptation, and conduct controlled pilot projects with partners before scaling. Given the increased regulatory oversight and interest, it would be helpful to negotiate with these vendors for access to AI model logic and outputs to enhance transparency. Note that these are often proprietary models, and vendors might resist providing full access. However, there is a middle ground that protects their intellectual property and gives you transparency. That will depend on the type and nature of the engagement and use case being deployed.	You want tailored solutions, but you lack the capacity to build them alone. You would benefit from integration and guidance.

Operating Model Decision Dimensions

For most AI initiatives, it is recommended to default to "buy" and "partner" to maximize resource efficiency and minimize risk. Reserve "build" for high-value situations where differentiation is crucial and internal capabilities warrant investment.

As shown in the following grid, for each business function, match the sourcing strategy to the complexity, available talent, and regulatory environment. While a firm's needs will differ from use case to use case, these are generally some dimensions to consider while choosing an operating model. (Please note this is not an exhaustive list, but rather a starting point.)

Criteria	Build	Buy	Partner
Initial Cost	High	Low / Medium	Medium
Time to Market	Slow	Fast	Medium
Need for Customization	High	Low	High
Complexity of Integration	High	Low	Medium
Talent	Required In-House	Low / Not Needed	Limited
Maintenance	In-House	Vendor	Shared
Compliance / Auditability	Must Build	Included	Depends

When evaluating how to incorporate AI-driven capabilities into existing processes and workflows, it is essential to consider the maturity of available solutions, the integration effort required, and your confidence in your teams' ability to execute.

For document intake and optical character recognition (OCR), purchasing established SaaS products is recommended. Such solutions offer reliable accuracy and natural language processing, enabling you to process documents efficiently with minimal integration challenges.

Chatbot adoption, particularly for policy administration or CRM, often involves buying or partnering with vendors that supply prebuilt AI bots. These AI bots can be further tailored to fit your firm's unique needs, enhancing customer service and operational efficiency.

Underwriting risk flags, which play a critical role in assessing application risk, benefit from partnerships with third-party analytics providers. These collaborations may require some customization to ensure the risk flagging models align with your firm's specific risk appetite and regulatory requirements.

Predictive modeling for mortality risk typically demands actuarial expertise and robust data science capabilities. Because most smaller firms lack this internal capacity, it is prudent to partner with specialized actuarial vendors that offer advanced modeling and analytics.

AI-augmented claims triage is increasingly available as a feature within modern core insurance systems and claims platforms. Buying these integrated solutions allows organizations to leverage sophisticated triage algorithms without investing in bespoke development.

Agent content personalization can sometimes be addressed internally. This is especially true for smaller-scale initiatives, and it can be accomplished by building on low-code platforms equipped with generative AI and prompt libraries. This approach empowers agents to tailor communications and recommendations to individual clients, improving engagement and satisfaction.

Each of these functions should be considered carefully within the broader context of your organization's strategy, resources, and regulatory requirements to determine whether building, buying, or partnering is the most effective path forward. (Again, for smaller firms, building should be viewed as a "last resort" option.)

Questions to Ask Vendors

When engaging with third parties for a "buy" or "partner" engagement, firms should ask the vendor questions that include:

1. Does your solution comply with NAIC Model AI Bulletin or equivalent regulations?
2. Can you provide explainability for your AI recommendations?
3. Do you offer integrations with our existing systems, such as PAS or CRM?
4. What data do we need to provide?
5. How is our data protected?
6. What is your cybersecurity posture and process?
7. What are you doing to protect your software against AI used to commit cybersecurity crimes?
8. What kind of training is needed for our users?
9. What are examples of other small carriers you have worked with?
10. Do you offer a free pilot or sandbox?

11. How often do you refresh your AI models?
12. How do you manage quality assurance and quality control?
13. What are the steps you take to prevent hallucinations?
14. What are the steps you take to prevent model drift?
15. What are the steps you take to mitigate bias?
16. What are the steps you take to reinforce the models?
17. What can we expect for product support?
18. Will you provide transparency around your AI models? How do you explain your models (explainable AI)?
19. Do we have token throttling with your product? If so, how is it metered and monitored? How will it scale?
20. Can you provide an inventory of your data sources? (depends on use case)

Arriving at the Operating Model

Firms can take the following action steps to arrive at an optimal operating model:

1. **Business Needs Assessment:** Identify priority areas where AI can drive efficiency or competitive advantage.
2. **Sourcing Strategy Selection:** Apply the evaluation checklist to determine the best path.
3. **Vendor/Partner Due Diligence:** Vet options using critical questions and require evidence of compliance and transparency.
4. **Pilot and Evaluate:** Run a small-scale pilot to test integration, performance, and business outcomes.
5. **Deploy and Monitor:** Roll out successful pilots broadly, with ongoing monitoring for bias, compliance, and ROI.
6. **Iterate and Scale:** Adjust strategies based on results, feedback, and emerging needs. Document each step to build an organizational AI playbook.
7. **Engage Your Leadership Team Early:** This ensures buy-in for sourcing decisions and alignment with business goals. Create a governance committee to oversee AI project selection, compliance, and vendor management. It is critical to invest in ongoing AI literacy and training for managers and staff. Finally, ensure that your teams document processes and lessons learned to refine your playbook for future initiatives.

3.2.5 Step 5. Vendor Governance

Most vendor AI features are now pre-packaged within vendor platforms, regardless of what kind of software platform is deployed in what part of the value chain (such as underwriting, claims, customer service, and fraud detection). Your firm's ability to steer AI adoption responsibly hinges on having a robust vendor governance process that should prioritize making oversight repeatable, scalable, and actionable.

Vendor governance matters because your organization often has limited transparency, in that sense that you rarely have access to the inner workings of vendor AI models. Regulatory accountability demands that even when using third-party tools, your company is responsible for downstream impacts. Unmonitored AI can introduce bias, errors, or reputational damage, and it can pose an operational risk, Therefore, it is vital that your vendor governance policies address these realities with proactive, structured controls. Your vendor governance policies can be "lightweight," but they need to be effective enough to enable a firm of your size to monitor, govern, and manage risks from AI embedded in third-party tools, platforms, or SaaS offerings. In this situation, you should instill "governance by contract and oversight by design."

Questions to Ask Vendors

During procurement or during annual contract reviews, you should ask the vendor questions that include:

1. Where is AI used in your platform?
2. What is the purpose of each AI feature? (For example, recommend, decide, or flag)
3. Can you explain how the AI model works to an underwriter or claims analyst?
4. What controls are in place to prevent bias or unfair treatment?
5. Can we test or simulate AI decisions before enabling them?
6. Can you share documentation for regulators if requested?
7. Do you maintain model update logs and performance reports?
8. Can we turn off the AI or override it manually if needed?

A Vendor AI Governance Model

To effectively oversee AI systems provided by external vendors, a structured approach is needed. It must ensure that technology is not only innovative, but also that it is transparent, fair, and compliant. While these principles apply to all forms of AI, model transparency and explainability might not be practically feasible for common generative AI vendor solutions. (See the concept of proportionality in the next section.) However, it is strongly recommended that firms follow these principles when dealing with "high-risk" AI systems.[3] There are generally five foundational pillars of this vendor AI governance model: Transparency, Explainability, Quality, Objectives, and Governance (Table 3).

[3] See LIMRA and LOMA AIGG AI Risk Classification (AIRC) Framework.

Table 3 — A Five-Pillar Model

Transparency	Maintain an internal AI inventory to ensure full visibility and oversight of all vendor-embedded AI in your organization.
Explainability	Vendors must provide clear documentation and tools to explain AI decisions, ensuring stakeholders understand how outcomes are reached.
Quality	Regular AI validation and monitoring ensures reliability, fairness, and ongoing compliance with performance standards.
Objectives	Monitor vendor AI's impact on business objectives by tracking outcomes and addressing issues to ensure value and alignment.
Governance	Ensure all vendor AI systems comply with regulatory standards and provide audit support, following industry frameworks for ethical and legal oversight.

Transparency

Transparency is the bedrock of responsible AI management. Your firm must have a clear understanding of where and how AI is deployed within all third-party platforms. This transparency is achieved by maintaining an internal AI inventory — which creates a "living, breathing" register that serves as a single source of truth to document every instance of embedded AI. Such a record provides leaders with the clarity needed to oversee complex digital ecosystems, anticipate potential risks, and ensure that no hidden or unauthorized AI applications escape notice.

Explainability

The principle of explainability and concept of explainable AI (XAI) underscores the importance of transparency in AI decision-making. Vendors should be able to articulate exactly how their AI systems reach conclusions or make recommendations. This is more than a matter of technical documentation, since it includes providing user-level transparency tools and clear, accessible explanations that foster trust among stakeholders. In practice, firms are encouraged to request thorough model documentation and insist on mechanisms that make AI reasoning visible and understandable.

Quality

Periodic validation of AI performance and fairness is essential to maintain system integrity and ethical standards. It is a non-negotiable that your vendor emphasizes regular testing and monitoring of vendor AI, using sandbox environments or test harnesses. These tools allow firms to assess system reliability, detect biases, and ensure that AI continues to meet performance expectations as it evolves in real-world settings.

Objectives

The goal of any AI implementation should be to deliver business value and meet business objectives. Monitoring the real-world impact of vendor AI is critical for aligning technology with business objectives. By tracking key business outcomes, such as underwriting consistency or rerouting customer calls to AI bots, your firm can evaluate the true value and effectiveness of AI solutions over time. Tracking objectives to expected outcomes helps quantify ROI and ensure that any unintended consequences are identified and addressed promptly.

Governance

Ongoing governance ensures that all AI deployments adhere to regulatory guidelines, requirements, and your internal risk thresholds. This includes alignment with frameworks such as NAIC guidelines and relevant state regulations.[4] Vendors should be expected to provide evidence of regulatory compliance and support for audits, enabling your firm to confidently navigate the complex landscape of legal and ethical obligations.

3.2.6 Step 6. AI Governance

It is vital for your organization to establish a "lightweight," but effective, structure for overseeing the ethical, compliant, and responsible use of AI — especially when AI is embedded in vendor platforms.[5] C-suite leaders must champion a rigorous, realistic governance process and institutionalize an actionable approach to embedding repeatable AI governance within the firm. AI governance should be predicated on five key principles (Table 4). By operationalizing these principles and embracing a repeatable, strategic approach, you can ensure that your AI initiatives deliver business value, while maintaining compliance, transparency, and stakeholder trust.

Table 4 — Key Principles for AI Governance

Proportionality	Apply proportional governance based on AI risk using LIMRA and LOMA's AIRC and AIRE frameworks to match oversight with system impact.
Shared Oversight	Cross-functional governance team with IT, Legal, Compliance, and business leaders distributes risk and breaks down silos.
Transparency	Track all AI systems and document where and how AI influences decisions and uses data.
Auditability	Require vendor audit logs and conduct regular AI reviews to ensure accuracy and compliance.
Human-in-the Loop	Require human review for high-impact AI decisions, documenting any overrides or interventions.

Proportionality

You must tailor the depth and rigor of your firm's AI governance activities to reflect the risk, scale, and complexity of each AI implementation. Not every chatbot needs a full audit, but anything influencing pricing, underwriting, or claims should be subject to elevated review.

For "low-risk" AI systems, such as simple chatbots used to respond to FAQs, this may be limited to periodic reviews and minimal documentation. Conversely, for "high-risk" AI systems — such as those that automate underwriting, pricing, or claims adjudication — rigorous, multi-layered governance with human oversight is essential. This includes comprehensive risk assessments, continuous performance monitoring, and regular third-party audits.[6] You would not assign the same level of risk and risk management strategies to every initiative, and using an established framework will provide a guide to aligning with industry standards.

[4] The LIMRA and LOMA AIGG has published an explainer for the NAIC Model Bulletin, the NIST AI Standard, and the NIST GenAI Standard.
[5] The LIMRA and LOMA AIGG has published an AI governance framework that can serve as a guide for your firm to adjust according to its size and needs.
[6] The LIMRA and LOMA AIGG has published an industry standard AI Risk Classification Model (AIRC Model), which allows firms to categorize each AI implementation by its level of risk. The AIRC is accompanied by the AI Risk Evaluation (AIRE) Framework, which also assists in evaluating AI implementations by a risk category.

Shared Oversight

Build a cross-functional governance team that includes IT, legal, compliance, and business line leaders. This distributes risk and ensures that multiple perspectives inform adoption decisions. In addition, it helps to break down cross-divisional silos that can be common in our industry. This team should meet regularly to review new AI initiative proposals, assess ongoing AI initiatives, review the AI landscape (including regulatory updates), and respond to emerging risks.

This shared oversight ensures that no single department dictates or overlooks AI deployment, and it integrates knowledge in technical performance, legal requirements, operational needs, and ethical considerations. Breaking down traditional organizational silos will help foster open communication, and it will promote informed, balanced decision-making by inviting a diversity of thought and experiences. The internal group's charter should outline roles and responsibilities, escalation paths for incidents, and procedures for onboarding or retiring AI systems — ensuring accountability and transparency throughout the AI lifecycle.[7]

Transparency

Your firm should build and maintain a dynamic, enterprisewide inventory of all AI systems. For small to midsize firms, this inventory likely would consist of AI solutions sourced from external vendors. With this approach, you should repeatedly document each AI utility's usage within your organization; the underlying business processes the tool supports; the data sources it leverages; the algorithms or models it employs (which you may not know with vendor solutions); and the decisions, outputs, predictions, or recommendations it produces. Your inventory should clearly identify the places in the workflow where AI is actively making or influencing decisions. It will be important to highlight data elements that are particularly sensitive (such as Sensitive Personally Identifiable Information and Protected Health Information.). Update this inventory in real time as your firm deploys new AI systems or retires/changes existing ones. The inventory not only supports internal accountability, but it also ensures readiness for regulatory audits or external inquiries — providing a single source of truth about AI activities across the firm.

Auditability

Embed explicit contractual obligations in all your vendor agreements with respect to their use of AI within their platform (either for building the platform or as functionality within the platform). Depending on the nature of the implementation and risk level, this contractual language might require comprehensive access to audit logs, detailed model documentation, an inventory of data sources, quality control and assurance mechanisms, testing results (including testing for bias), steps the vendor takes to prevent and mitigate hallucinations, human-in-the-loop protocols, governance mechanisms, and a running manifest of model updates or changes. In addition, you should leverage your internal AI Governance Group/Committee to establish robust protocols for periodic audits of all medium-risk and high-risk systems.[8] For medium-risk and high-risk systems, expect to conduct regular sampling and testing of outcomes to verify accuracy, fairness, and reliability.

It will be important to create standard operating procedures for investigating anomalies or errors, such as unexplained decisions, performance degradation, or customer complaints attributed to AI output or decisions. Your firm must diligently maintain meticulous documentation of all audits, corrective actions taken, steps taken to mitigate future issues, and lessons learned. These practices not only demonstrate due diligence to stakeholders and regulators, but they also build internal confidence in the robustness and trustworthiness of your AI ecosystem.

[7] See LIMRA and LOMA AI Governance Group AI Project Lifecycle (AIPL).
[8] See LIMRA and LOMA AI Risk Classification Model (AIRC Model).

Human-in-the-Loop

The stakes have grown considerably for decisions associated with using AI to automate predictions or outputs. In high-impact scenarios, it is critical to ensure that human subject matter experts maintain oversight and retain the authority to challenge, review, or override AI-generated outcomes. The terms "human-in-the-loop"or "human-in-the-center" are used quite often in the context of AI.

Human-in-the-loop simply means that qualified humans (domain experts or subject matter experts) stay involved to govern and control all facets and steps where AI makes consequential decisions — especially those that impact people's lives. The outcomes can directly affect humans (including the wellbeing of employees, customers, or other stakeholders), impact your brand and reputation, increase legal risk or exposure, impact regulatory standing, detrimentally affect financial outcomes, harm your reputation, or adversely influence your firm's strategic direction.

Consequential AI decisions, therefore, require a heightened level of scrutiny and accountability. Human-in-the-loop ensures that AI-driven automation is balanced by human judgment, expertise, and ethical consideration, and that it reflects your corporate values. By operationalizing clear policies, workflows, documentation, and training, organizations can unlock the benefits of AI while safeguarding against unintended consequences. Robust governance not only protects the organization, but it also nurtures stakeholder trust, supports regulatory compliance, and advances responsible innovation.

Human-in-the-loop ensures that employees can review, approve, or override what the AI suggests, so that AI never acts completely on its own where it matters most or where you have most exposure. Firms should institutionalize safeguards that ensure domain experts such as underwriters, claims specialists, legal counsel, or compliance officers retain the authority and responsibility to review, challenge, or override AI-generated decisions as appropriate (for medium-risk or high-risk systems). You must clearly define which types of AI recommendations require mandatory human review before final action and integrate these checkpoints into business processes and operational workflows. This is especially vital as you work with vendors that provide AI solutions. The human expertise should reside within *your* firm.

As previously stated, depending on the AI use case and type implemented, you should institutionalize the need for thorough documentation of every instance where human intervention occurs, including the rationale for the override and any subsequent changes to policy or process. Codify the requirement for human review in high-impact or sensitive decisions. For example, ensure that underwriters or claims specialists have final authority to override or question AI outputs, and document all such interventions for the future.

Steps to Achieve AI Governance

The following grid reviews the major steps involved in developing AI governance within your firm.

Step	Actions
1. Prioritize Proportionality With the AIRC and AIRE Models	• Begin by cataloging all current and planned AI applications, including those provided by vendors. For each, perform a risk assessment using the AI Risk Classification (AIRC) Model. • Utilize the AI Risk Evaluation (AIRE) Framework to determine the appropriate level of oversight and controls for each AI project. For instance, an underwriting automation tool may require full documentation, ongoing model validation, and periodic external audits, whereas a simple chatbot may only need basic monitoring. • Document risk categories, oversight requirements, and mitigation strategies. Store these in an AI catalog that is routinely reviewed and updated.
2. Build Shared Oversight and Break Down Silos	• Form a cross-functional AI governance group comprised of IT, legal, compliance, and business unit representatives. Ensure participation from senior leadership to signal commitment. • Establish monthly or quarterly committee meetings focused on reviewing new AI initiatives, risk assessments, compliance updates, and incident reports. • Use collaborative platforms to share documentation and solicit feedback, enabling distributed teams to contribute insights and stay informed.
3. Achieve Total Transparency Through a Comprehensive Inventory	• Develop a dynamic AI inventory system that captures all AI applications, both internally developed and vendor-supplied. • For each entry, record its purpose, deployment status, data inputs and outputs, decision-making role, risk rating, and associated business owner. • Update the inventory every quarter and whenever a new AI tool is added or a significant change is made. Make the inventory accessible to all relevant teams for maximum transparency.
4. Enforce Auditability and Vendor Accountability	• Negotiate contract clauses with vendors mandating disclosure of model changes, access to audit logs, and support for regulatory reviews or incidents. • Conduct internal audits at least annually on high-risk AI systems, reviewing outcomes, data usage, and compliance with documented policies. • Create a protocol for investigating anomalies, errors, or complaints related to AI outputs, with a clear escalation path to the governance committee and executives.
5. Embed Human-in-the-Loop	• Define explicit scenarios in which human review is mandatory — such as underwriting denials, potential claims denials, or fraud alerts. • Train business users on when and how to override AI decisions, and require documentation of every intervention for future analysis and compliance reporting. • Leverage the AIRE framework for best practices and case studies to reinforce the importance of human oversight.
6. Operationalize Governance Across the Organization	• Focus intensive governance efforts on applications flagged as medium-risk or high-risk. Assign an AI Oversight Lead, typically from IT or Innovation, to coordinate activities and maintain the governance register. • Appoint outside experts or engage third-party advisors to support the governance process. (This especially applies to smaller carriers with limited resources.) • Establish incident management protocols for timely reporting, escalation, and resolution of AI-related issues. Document every incident, root cause analysis, and corrective action taken. • Deliver targeted training for all staff on the company's AI Use Policy, emphasizing ethical use, data privacy, and the importance of transparency.

Steps to Achieve AI Governance (continued)

Step	Actions
7. Proactively Monitor Regulatory and Policy Changes	• Schedule quarterly reviews of regulatory bulletins from NAIC, state Departments of Insurance, and consumer privacy laws. Update internal policies and governance practices in response to new regulations. • Assign responsibility to the legal or compliance team for tracking changes and disseminating updates throughout the organization. • Engage with industry peers and resources for ongoing education, benchmarking, and shared best practices.
8. Drive Continuous Improvement and Strategic Reassessment	• Review the effectiveness of AI governance at least biannually, leveraging performance metrics, user feedback, and audit results. • Solicit feedback from business users after every major AI deployment or upgrade, and use these insights to refine policies and controls. • Update the AI Use Policy annually, incorporating learnings from internal reviews and industry standard revisions.

Operationalizing AI Governance

Consider the following recommendations when operationalizing AI governance within your organization:

i. Focus most your efforts on the governance of medium-risk and high-risk AI systems. These AI implementations have the potential to directly impact humans (customers), cause regulatory issues, create financial issues, or harm company reputation.

ii. Create a cross-functional AI group. Often known as an AI Governance Group or AI Committee, this team includes individuals from across your value chain, representing areas including IT, legal, compliance, business lines, and operations. Designate a lead for this group. (The lead is often an IT person.) Consider leveraging outside experts to augment areas where you do not have the resources. Leverage tools and resources for LIMRA and LOMA members, as well as those provided by the LIMRA and LOMA AIGG.

Your firm must have an AI and/or GenAI Safe Use Policy. Regulators increasingly expect to see these as they ask for an enterprise AI governance framework.[9] These industry-standard policies outline acceptable use, oversight requirements, and employee responsibilities when it comes to AI. You may choose to use the LIMRA and LOMA AIGG AI Use Policy as a starting point and then adjust it with customizations and annual updates to reflect regulatory, business, and technology changes. Ensure that you are tracking changes to the industry standard template as well. It is also critical to deliver targeted training to prepare all employees to interact with or rely on AI outputs. Continuous improvement should be a cornerstone of your AI governance plan and a focus for your AI Governance Committee — including a review of your AI inventory and governance effectiveness at least twice per year. Depending on the use case and type of AI, this group should proactively solicit feedback from users after major AI implementations and updates.

This AI group should also regularly monitor the regulatory landscape. The NAIC Model Bulletin meticulously maps all AI use cases to relevant regulatory guidance for AI implementations across the value chain.[10] As state Departments of Insurance release new or updated requirements for AI explainability, fairness, or transparency, your firm must to be vigilant in identifying changes that can impact you. It is strongly recommended that this group also pay attention to data privacy laws.

[9] Leverage the LIMRA and LOMA AIGG Corporate AI Governance Policy and the GenAI Use Policy templates.
[10] The LIMRA and LOMA AIGG has published explainer guides for the NAIC Model Bulletin, NIST (National Institute of Standards and Technology) AI Standards, and GenAI Standards.

iii. Develop a holistic AI inventory as described earlier, and use it to track every AI-enabled tool in use across the enterprise, diligently logging the business purpose, risk classification, data inputs, and outputs.

iv. Take your vendor management protocols seriously, reviewing contract language and formalizing language around AI used in vendor products. Your contract clauses should require vendors to disclose use of AI, provide proactive communication and testing results from AI model updates, and provide the right to audit AI operations and outcomes for medium-risk to high-risk AI systems (see Proportionality). Set expectations for vendor support during regulatory inquiries or incidents by establishing clear, mutually-agreed-upon incident management protocols. (You may already have some of this infrastructure in place for system outages, cybersecurity incidents, and other situations.)

For AI in particular, you must co-create a process for reporting, escalating, and tracking resolution of AI incidents, regardless of the cause of the incident (which can include errors, hallucinations, unexpected outputs, and infrastructure failures). It should be expected, and documented in clear language, that any incidents need to be closed out with appropriate root cause analyses and corrective actions, as you would do with outages and cybersecurity issues.

3.2.7 Step 7. Change Management

Change management, as with any new technology, is going to be critical to your AI implementations and adoption. C-suite leaders should proactively manage the organizational, cultural, and behavioral changes that come with AI to secure adoption, build trust, and achieve long-term success. There are five essential principles for effective AI change management:

1. **Prioritize Clarity Over Complexity.** Explain what AI is doing in simple, relatable terms. Consider a broad communication strategy, but also personalize the message to teams and/or individuals on how AI will benefit them and how they do their jobs.

2. **Inclusivity Will Drive Adoption.** Engage your enterprise at all levels and across the value chain for successful AI adoption. Bring employees, and business users specifically, along with you for the journey — not just relegating AI strategy discussions to IT and/or third-party vendors.

3. **Transparency Builds Trust, and Trust Nurtures Transparency.** You must share your AI goals, how these AI enablers further business objectives, the current and planned capabilities of the platforms, known challenges, risks, and risk mitigation — and invite employees to help you capitalize on opportunities and mitigate risks.

4. **Celebrate All Wins.** Highlight early wins visibly and vocally. Even the smallest wins can generate enthusiasm and momentum, helping employees to rally behind AI implementations.

5. **Fears Foster Failures.** Do not underestimate the need for change management. You must address employee concerns about job security, skills, and reskilling needs, as well as how their specific tasks and/or jobs will change due to AI. If you do not yet have all the answers, then be transparent and acknowledge that you do not know, but do not dismiss these concerns.

When embarking on your AI journey, again, prioritize clarity over complexity. C-suite leaders have a unique responsibility to ensure that every AI initiative is described in accessible language that employees can understand. If they do not understand it, then they will not adopt it. And if they do not adopt it, then there will be a potentially vocal minority that could derail the AI implementation. Rather than relying on technical jargon, focus on the value your firm seeks to achieve from AI.

Your communications should focus on how AI improves business outcomes. When discussing the productivity and operational efficiency gains from AI, take caution that referencing lift in productivity could be perceived to mean potential job displacement. Reframe this message to be about the positive outcomes a productivity lift could create for employees. Frame the business benefits the firm would gain — such as saving time, reducing costs, and boosting productivity — but remember to also focus on what it means for every employee. For instance, individual staff members may have the opportunity to reinvest their time in training and learning new skills; others may be able to take on "stretch" initiatives and assignments. Ultimately, your leadership team plays a critical role in cascading and personalizing the messaging to employees. Your cross-functional AI group, which represents the entirety of your organization, also can be ambassadors for change and voice the diverse perspectives of their individual business units.

Effective communication around AI-driven change will greatly help to foster transparency and develop trust. Transparency is the bedrock of trust, and for your firm to build that trust, C-suite leaders must openly communicate their AI goals and how they will benefit the organization. Employees should feel empowered to ask questions and express concerns, perhaps through regular "AI open office hours" or interactive sessions where leaders and project teams listen and respond in real time.

In addition, the leadership team must prioritize celebrating early wins. Every successful AI implementation, regardless of how modest it is, generates "buzz" and creates momentum. Even a small pilot program that saves 30 percent of time in executing a task should be celebrated as a milestone. This will help your firm build energy and enthusiasm around AI and encourage employees to lean in and drive adoption. There continues to be significant anxiety around AI, and this will likely increase with the emergence of agentic AI and AI agents.

Employee concerns around AI typically relate to job security and displacement, as well as anxiety about how their jobs will change and whether they will have to learn new skills. An effective change management strategy requires proactively addressing these concerns. Communications with employees should focus on how AI can be viewed as "augmented intelligence," designed to support their roles, not replace them. Reinforce your firm's commitment to upskilling and role enhancement. Education and AI literacy will go a long way to demystify the technology and reduce the fear of the unknown.

Key Messages for Core Constituencies

The following grid suggests key messages that core employee groups would need to hear about AI plans.

Constituency	Key Messages
Executives	AI is a business enabler that can help us reduce costs, increase revenue, and achieve growth. It is not just a technology for technology's sake; it must be clearly anchored to our business objectives and deployed to further our enterprise goals. The executive team sets the tone on how successfully our firm can adopt AI within our business operations. Your teams will be concerned about job displacement. It is your responsibility to position AI as "augmented intelligence," a technology that will help each of us delegate rote, repeatable, and operational tasks to AI — and ultimately become more productive. Frame AI as a business accelerator. Explain how it reduces operational costs, drives competitiveness, and positions the company for future growth.
Managers	Managers have to be vocal champions for change and advocates for using AI safely, effectively, and ethically. Each manager will be responsible for change management — reimagining existing business processes and considering how AI can help them become operationally efficient — as well as stewardship of how employees actively use these tools.
Business Units	Stress that AI will automate tedious tasks, allowing professionals to focus on nuanced, high-value decisions. Reassure them that their judgment remains central to the process. AI will not replace your judgment. The human-in-the-loop concept relies on your skills and experience. You must use AI to automate your routine tasks, but ensure that you are using it in a safe, effective manner and in compliance with our enterprise policy. It is important to critically reexamine your business processes and consider how AI can help make them more efficient. It is also vital that you adopt a continuous learning mindset, where you are unafraid to experiment and innovate responsibly.
All Employees	We are bringing in tools that can automate, assist, and scale, but rest assured that we are proceeding methodically and with intention. AI will never be able to replace our soft skills and core corporate values. We encourage you to pursue relevant professional development programs that will help you learn to leverage AI in a powerful manner. Incorporate themes from the following grid on common concerns, and address them proactively in your communications.

Responses to Common Concerns

Common Concern	Response
"Will AI replace jobs?"	*No. AI is here to enhance and augment your role, not eliminate it. We are using AI to reduce repetitive tasks so you can focus on what matters most. AI is a tool to "free up" employees for creative, strategic, or personalized work. Our company is commited to upskilling and role enhancement.*
"I do not understand how it works."	*You do not need to have an in-depth understanding of how AI works, just like you would not need to know the inner operations of most complex household appliances. We will provide simple explanations and resources for you to educate yourself. While learning resources will be available, rest assured that technical mastery is not required for day-to-day use.*
"Can I trust AI?"	*Every AI tool we use will rely on the human-in-the-loop concept. Higher-risk systems will have the ability for human overrides, and testing and controls will be built into our business processes. We will share audit results and improvement plans regularly.*
"I am not technical."	*You do not need to be technically inclined. Most tools are embedded in software you already use. You are a domain expert, and we will rely on your expertise to continuously make AI better. Think about AI like a new college hire or an intern who needs training and mentoring. AI tools are designed to be user-friendly and are embedded seamlessly in familiar workflows. We will provide ongoing support and encourage feedback.*

Change Management Actions to Consider

Consider taking the following actions to help your firm's change management approach to AI:

1. **Leadership Endorsement.** Issue a CEO statement, host a town hall, or publish a policy memo on the company's AI vision and responsible use. Visible leadership sets the tone and signals organizational commitment.

2. **Use Case Showcases.** Schedule regular "AI in action" demos. Rotate presenters from different business units to highlight real-world applications and encourage staff to share feedback.

3. **Office Hours for AI.** Organize drop-in sessions where staff can ask questions, see demonstrations, or discuss concerns with project leads and vendors. This fosters transparency and hands-on learning.

4. **Simple AI Onboarding Kits.** Develop concise, accessible materials for each new AI feature, such as straightforward guides or explainer videos. Distribute these well ahead of rollout and update them based on user feedback.

5. **Advocates Network.** Select "AI ambassadors" from business teams to act as liaisons, gather peer insights, and support training. Empower these champions to be visible advocates for AI adoption.

3.2.8 Step 8. Talent Strategy

For small to midsize firms, the talent strategy related to AI is less about assembling a large team of IT professionals, data scientists, and AI engineers — and more about cultivating a culture of AI literacy and pragmatic partnerships. These partnerships likely can be an expansion of existing partnerships with third-party vendors. The basis of an AI talent strategy for small to midsize carriers should not be based on massive hiring initiatives or expensive technical overhauls. Instead, it involves more of right-sizing the approach to maximize impact with the available resources and strategic augmentation. Your AI talent strategy should ensure that you can adopt and scale AI, despite not having in-house data scientists or AI engineers, by creating a right-sized blend of internal roles, reskilled and upskilled staff, and external support.

There are generally five foundational pillars of this AI-driven talent strategy (Table 5).

Table 5 — Key Principles for an AI-Driven Talent Strategy

Redefining Team	Empower AI-literate leaders across the business to bridge operational needs with external expertise for effective adoption.
Filling Roles	Blend internal AI champions with strategic external advisors to maximize expertise and context for effective adoption.
Upskilling	Empower staff with practical AI skills using no-code tools and accessible training to drive effective adoption.
Partners	Partnering with external experts and vendors enables smaller carriers to access AI talent and resources efficiently.
Governance	Internal cross-functional committees, informed by external expertise, provide governance that aligns AI talent strategy with evolving regulations, ethics, and business priorities.

Redefining the "AI Team"

The common misconception is that meaningful AI adoption requires a dedicated in-house team of highly specialized experts. For small to midsize firms, this is neither feasible nor realistic. Most of all, it is not necessary. For these carriers, AI implementation successes depend on empowering business decision-makers and core operational staff to understand AI's capabilities, opportunities, risks, and limitations. They must grasp how AI enables your corporate business objectives and act as informed liaisons with external third-party partners.

Essentially, you do not need a department of IT professionals who are AI model developers and data engineers. Rather, you need "AI-literate" leaders who can champion responsible AI adoption. A fundamental aspect of being an AI-literate leader is to clearly understand your own capabilities and recognize when to seek outside help and expertise.

How does this translate to your definition of an internal AI team? It requires a focus on identifying and upskilling those employees who demonstrate curiosity and a willingness to innovate and ideate. These individuals are unafraid of "failure" and recognize the value of a minimally viable product. They are very disciplined in "starting small" and will not let perfection be the enemy of good. They can navigate ambiguity with confidence and do not let the prospect of one initiative not meeting its goals dissuade them from moving forward with the next innovative idea.

Equipped with the right foundational knowledge, these AI ambassadors can serve as mediators and translators between your business and operational needs and how technical possibilities can address them. It is important that they have an understanding of the business because only via their deep understanding of insurance operations and your organization will it be possible to evaluate, pilot, and embed vendor AI solutions. These domain experts should enrich and be entrenched in domain knowledge via pursuit of relevant professional development programs and designations.

Filling Key Roles

Specialization is important when it comes to AI, but this does not always require a full-time employee. For instance, while someone should have subject-matter expertise in AI (such as with AI strategy or regulatory and compliance updates), that person does not need to be a dedicated, full-time resource.

Several small to midsize firms leverage outside CIOs and/or CTOs, external consultants, or part-time external legal counsel who monitor the impact of evolving AI regulations and regulatory frameworks. These resources can leverage their depth of subject expertise and guide you accordingly, and your organization will not need to build this expertise in-house. Alternately, for some of these roles, you might have one in-house individual who can have multiple responsibilities related to AI.

The key is to creatively blend internal staff (both subject matter experts and simply enthusiasts willing to learn) with external advisors, ensuring that your firm's voice and context remain central to any AI implementation. For example, your AI compliance lead might be your in-house regulatory and compliance point person, who can partner with outside legal counsel as needed. Or your AI product owner could be your existing leader of underwriting, who sees how AI can augment underwriting tasks and guide accelerated underwriting-type AI use cases. This person would ensure that outputs align with everyday workflow realities, comply with your firm's underwriting rules, and remain compliant and transparent.

Upskilling and Reskilling

Upskilling and reskilling your teams is key to implementing any successful AI strategy. The most effective AI adoption strategies focus on teaching core teams how to use the AI tools you provide. Without educating employees on AI fundamentals, demystifying concepts, dispelling common myths, and increasing their comfort level with the tools, your AI strategies will not

gain traction. Educating employees on AI is just as vital as upskilling and should be considered table stakes. Without an AI-literate workforce, it will be impossible to skill, upskill, or reskill staff.[11]

While many free or low-cost AI training and education resources are available, C-suite leaders should be judicious in choosing which training programs to recommend to their teams. Focus on fundamentals and then supplement these educational modules with practical, scenario-based learning. This will help employees become more comfortable experimenting and iterating.

The following grid includes some common, recommended tasks C-suite leaders should incorporate when executing an AI-fueled talent strategy.

Conduct Periodic Skills Gap Analyses	Start with a structured assessment of existing technical and non-technical skills across the organization.[12] Map current employee competencies to the requirements of emerging AI-enabled and AI-augmented functions, tasks, and roles, ensuring that training investments are precisely targeted.
Promote Enterprise-Level Learning	Encourage employees from various divisions to engage and actively participate in AI learning modules. Cross-functional teams foster creative problem-solving and ensure that AI adoption is not siloed, but instead that it drives holistic transformation. Collaborate with academic partners and industry-specific resource providers.
Build AI Champions	Identify AI enthusiasts, early adopters, and naturally curious team members to become "AI champions." Choose those with some level of domain expertise so they can align AI's capabilities with specific business problems your firm is trying to solve. Equip them with training and ask them to mentor their peers. This will foster a self-sustaining culture of AI literacy throughout your organization.
Leverage "Bite-Size" Learning	The way employees learn — especially Generation Z and Generation Alpha individuals — is dramatically shifting. Rather than only offering lengthy courses, incorporate microlearning (short, focused modules) into daily workflows. AI can personalize these modules based on employee progress and role, ensuring relevance and sustained engagement. Keeping with the shift in learning preferences, consider using gamified platforms that reward learning milestones, offer leaderboards, and simulate real-world AI scenarios. This approach increases motivation and helps teams experience the tangible benefits of AI in a risk-free environment, while bringing your organization together around a common purpose.
Integrate Soft Skills	AI will be able to automate a lot of things, but it will struggle to automate soft skills. Soft skills development, especially with newer generations, will be vital. These include values, ethics, judgment, change management, and communication skills.
Continuous Improvement	Use AI-driven feedback tools to provide employees personalized suggestions for improvement as they progress through their reskilling journeys. This mindset will be critical to ensure employees do not view skilling and reskilling as a "one and done" event. Establish key performance indicators for your AI-based skilling programs, including standard measures such as adoption rates, productivity improvements, reduction in manual tasks, and employee satisfaction. Measure and evaluate these regularly at a frequency that fits your organization. You know your firm best. If you measure too soon or too frequently, you may not see a measurable uptick in value. On the other hand, if you measure too infrequently, you will not be able to enact any necessary changes quickly enough.

[11] The LIMRA and LOMA AIGG provides deep industry-specific insights on AI. From a talent perspective, its AI Automation Identification Framework may be a helpful tool. Across your value chain, it allows you to go through each role and identify the tasks within the job that can be automated using AI. Therefore, you will be able to outline the jobs of the future and a re/skilling strategy for each of them.
[12] Consider using the LIMRA and LOMA AIGG's AI Impact Assessment Framework as a guide.

Pragmatically Leveraging Partners

If needed, your firm can leverage outside technology leaders, such as CIOs, CTOs, and Chief AI Officers. These resources can provide accurate, timely, and up-to-date information, while advising you on AI strategy, architecture, and vendor selection. Effectively serving as thought partners and practical guides, specialized consultants can be brought in to address pressing challenges and help steer major AI implementations. You also can engage legal experts, particularly those with a grasp on evolving AI regulations, on a retainer or per-project basis to ensure ongoing compliance and anticipate regulatory changes.

Your firm also has ready access to a vast ecosystem of Software-as-a-Service (SaaS) providers. These vendors allow you to implement and scale AI implementations with minimal IT investment. Your business units would be able to experiment, pilot, and implement AI use cases directly relevant to their processes and operational workflows. As discussed earlier, it is imperative to include language in your vendor contracts — and any new RFPs when selecting AI vendors — to ensure that AI implementations are transparent, auditable, and aligned with firm's risk profile and core values.

Participation in AI governance groups can open doors to shared research, benchmarking studies, and collective learning and execution on matters such as AI ethics and standards. Another resource to consider is regional universities and technical schools. These academic institutions might provide access to academic expertise, joint research initiatives, and a pipeline of emerging talent through internships or specific partnered projects. They likely are seeking opportunities to provide their students real-world business exposure, and you would benefit from fresh ways of thinking and innovative approaches to AI and digital transformations. It can be beneficial for your existing subject-matter experts to collaborate with individuals who take fresh approaches.

C-suite leaders should consciously adopt a holistic ecosystem approach. Allow your partners to help you. It will enable you to amplify your internal strengths without sacrificing agility or incurring unsustainable costs. Blend internal domain knowledge and subject-matter expertise with the precision and depth of external specialists to allow your firm to remain nimble, innovative, and responsive to the rapid changes in AI technology and the regulatory landscape. It will democratize AI access for your firm and foster a culture of partnership and continuous learning. This type of approach will help your firm confidently navigate the evolving insurance landscape, while shaping AI implementations to fit their unique needs and business goals.

Governance

A strong governance framework is foundational to an effective AI-driven talent strategy. This framework typically combines internal oversight with strategic collaboration. Your internal AI Governance Committee should be responsible for setting AI guidelines, prioritizing use cases, and monitoring ethical considerations. This committee will be expected to work closely with external advisors to ensure that internal policies remain current with industry standards and evolving regulations.

Governance is also about fostering a culture of responsible AI use, encouraging transparency in decision-making, documenting workflows, and regularly reviewing outcomes for fairness and compliance. From a talent strategy perspective, AI governance will be overseen by this small internal committee with shared accountability. The delivery of AI use cases is typically co-owned by the business and executed by vendor partners. AI risk review involves compliance leads and external legal advisors. Change management and upskilling are coordinated through internal communications and human resources, supported by ongoing learning sessions and accessible online resources.

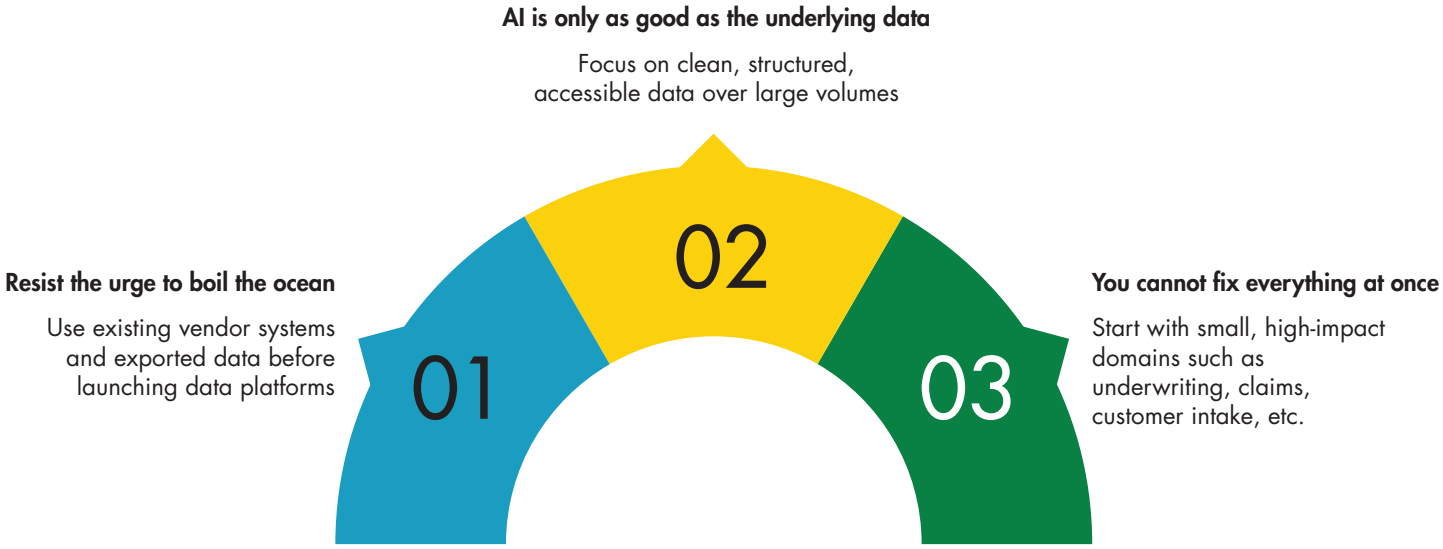
In addition to its core oversight functions, the internal AI Governance Committee should take an active role in fostering AI literacy throughout the organization. This includes helping to identify and potentially contribute to the development of educational initiatives that demystify AI for all employees, equipping them with the foundational knowledge needed to engage with AI implemented within your firm. The group should proactively identify areas where skilling and reskilling can make the most impact, championing learning pathways tailored to different roles and levels of expertise. By organizing workshops, curating online resources, and facilitating peer learning sessions, this cross-functional group can empower their colleagues to confidently use AI tools integrated into business processes.

Their guidance ensures that employees recognize practical opportunities to leverage AI, enhancing not only operational efficiency but also professional growth. Employees will trust these individuals more than they would outside consultants, since they are their fellow employees, just as subject to AI-driven changes as they are. Through this commitment to education and enablement, your internal AI Governance Committee should help cultivate a workforce that is adaptable, innovative, and prepared to maximize the value of AI.

3.2.9 Step 9. Data Management

Even with a "buy" or "partner" approach to your AI implementations, your firm cannot achieve AI success without focusing on your enterprise data. This is particularly true of AI solutions that use your enterprise data for an output, whether that output is an AI prediction or recommendation. Your firm would benefit from a data management strategy with or without AI, but this is of particular importance in the age of AI. You simply cannot have good AI with bad data. There are three central tenets for C-suite leaders to keep in mind when it comes to data management (Figure 3).

Figure 3 — Central Tenets for Data Management



In our mature industry, historically we have not treated data as an asset — choosing to treat it as a byproduct of our systems, rather than a product. Data integrity, availability, quality, efficacy, lineage, and security are prime concerns. In any given carrier, data can be somewhere, anywhere, and nowhere concurrently. This is a major challenge for our industry to overcome.

While establishing a full-scale data strategy and governance program may not be realistic for small to midsize firms (since these demand time, attention, and resources), data stewardship should be integral to your operations. By focusing on clear ownership, retention alignment, privacy controls, robust vendor terms, and ongoing bias monitoring, C-suite leaders can establish a governance framework that is practical, actionable, and ready for AI. Your data management should start small, allowing you to scale with discipline. It will be important to adapt data management to evolutions in your business and AI itself.

The following are some ways to establish a data management program:

Data Stewardship and Ownership

Effective data governance starts with clear ownership. Begin by appointing a responsible data owner for each core business domain across your value chain (including underwriting, claims, service, marketing, and so on). This individual should understand both the operational workflow and the data that powers it.

Be intentional about how you frame the conversation with these designated individuals, referring to them as "data stewards" instead of "data owners." The former implies a progressive champion, while the latter implies being "stuck" with additional responsibility. Create a simple matrix listing domains and the assigned data stewards. Review this periodically, and update it as needed, especially as roles shift or new initiatives are launched.

The responsibilities of data stewards include:

- Maintaining an inventory of all data sources and fields relevant to their domain
- Monitoring data quality and reporting inconsistencies or gaps
- Serving as the point of contact for vendor questions, audits, or AI implementation teams
- Championing clean data and compliance within their functional area

Data Quality

Data quality always has been of paramount importance within our industry. However, this will become an acute and pressing concern as your firm expands its AI footprint. AI thrusts the importance of data quality sharply into focus. Reliable AI decisions depend not just on the volume of data, but on the cleanliness, accuracy, and traceability of the underlying data. Data stewards hold a unique position to champion quality, efficacy, and lineage across the enterprise, often since they are the overseers of upstream systems and business processes.

To elevate and champion data quality, data stewards must:

- Define what "good data" means for every critical business process and within each data field that supports it. For instance, if a data field for the face amount of a policy is $1.00, you know immediately that it is bad data within that field. Ensure that third-party vendors leverage your subject matter expertise and use validation rules and automated

checks to catch errors at the source. The worst thing firms can do is "fix" data at the destination. Data stewards must establish clear standards for data entry and maintenance.

- Own data lineage — often known as data provenance — from creation to consumption, by keeping records of how data flows, transforms, and is used by downstream AI, reporting, business intelligence systems, and analytics. This clarity helps address compliance queries and root-cause analysis.

- Data stewards should engage regularly with other stakeholders to review data maps, address gaps, and ensure interoperability between systems. They must collaborate across business units, IT, your internal AI Governance Committee, and vendor teams.

- Data stewards should schedule routine evaluations of data, not just for accuracy, but also for relevance and timeliness. They must encourage feedback from users within their business unit to identify stale or misleading inputs. In doing so, they will be able to promote efficacy through ongoing data audits.

- Data stewards must be active champions of transparency and documentation. They must consistently document data definitions, transformations, and quality checks within the scope of the business units and underlying systems they represent. They should make this documentation accessible to both technical and business users so they can comprehend and trust the data driving AI decisions.

- Data stewards should celebrate improvements and share lessons learned across teams to build a culture where clean, effective data is everyone's responsibility.

Data Governance

AI initiatives must comply with several data-related regulations and regulatory and compliance requirements. These include established records retention schedules. C-suite leaders should ensure that any data sent to a vendor for model training, testing, or production AI applications is not kept longer than permitted. This includes both structured records (such as databases and spreadsheets) and unstructured data (such as scanned documents and emails). Firms should diligently map all AI project data sources against their records retention schedule. To do so, work with your internal compliance or audit teams and/or your external counsel. Data stewards should flag datasets that are approaching expiration and set reminders for deletion or review. Implicitly, they will be responsible for working with counsel or compliance-type resources and teams.

To effectively stay on top of records retention schedules, data stewards should:

- Audit data used in AI implementations to confirm retention dates and permissible use.

- Implement automated deletion routines for expired data, or establish manual reviews for small datasets.

- Document any retention policy exceptions, such as regulatory holds or litigation-related preservation. Pay particular attention to HR, legal, and finance datasets.

- Train staff on the intersection of AI use and retention rules, especially when handling backups and data exports.

An additional facet of data management is data privacy and protection. Absent federal legislation on data privacy, state-based data protection regulations have to be considered. Before using any data outside of live production (for example, for AI model development, vendor demos, or internal testing), your firm must ensure that all personally identifiable information (PII) and Sensitive PII are masked, anonymized, or excluded. The data steward can also serve as your designated data privacy champion, accountable for overseeing these controls in all AI-related activities.

Data stewards should:

- Use, or ensure your vendors use, automated data-masking tools or scripts to redact PII from AI training data datasets.
- Establish a checklist for staff to verify removal of PII before sharing data with vendors or external consultants.
- Partner with vendors to audit their non-production environments for accidental exposure of PII and respond quickly to any findings. Perform spot audits on a regular basis to reinforce best practices. (This will need to be documented in your vendor contracts. Also note that not every vendor will be willing to "open their doors" as they seek to protect their intellectual property.)
- Clearly document which fields are considered PII, and educate employees by providing examples.

Data stewards also should be diligent to ensure the partner vendors that consume your data (as well as other datasets) do not use your proprietary data without your explicit consent. Third-party vendors may request access to your data for AI services, but data stewards, supported by the C-suite, must safeguard your organizational and customer information. You should insist on contractual clauses that prohibit vendors from using your data to train their own models or for any purpose unless they have your explicit, written consent.

In keeping, your firm must:

- Maintain a centralized log of vendor agreements, which is reviewed at least annually for compliance and updated as AI capabilities evolve.
- Review all vendor contracts for language regarding data use, model training, and data ownership.
- Negotiate for clear audit rights to confirm vendor compliance.
- Require written attestation from vendors on data use before onboarding and annually.
- Establish a process for reporting and remediating suspected misuse.

Monitoring for bias is also a key facet of data governance. Your firm is responsible for monitoring whether data used in AI creates skewed or discriminatory outputs. AI can unintentionally perpetuate or amplify biases that can be present in data. Your firm must make the act of bias monitoring a routine aspect of AI deployment.

This means data stewards must:

- Work with vendors to regularly test models for disparate impact against protected groups and classes. Schedule and conduct regular reviews for active AI implementations as appropriate.
- Implement feedback loops with business users and their divisions, as well as compliance teams, to flag unusual outputs that seem suspect. This is a prime example where business subject matter expertise matters deeply.
- Work within their own business unit and across business units with other data stewards to diversify datasets and remove any suspected bias.
- Document all bias audits and corrective actions taken in partnership with the vendor for regulatory review.

3.2.10 Step 10. Scaling and Continuous Improvement

C-suite leaders must develop processes that allow for the expansion, improvement, and adjustment of their AI implementations to ensure the long-term success of AI strategies. Firms should institutionalize a mindset that each and every new AI use case and implementation is both a learning opportunity and a chance to strengthen your organization's overall AI strategy.

Following are some factors to consider as you seek to operationalize, scale, and continuously improve your AI programs:

Tracking and Improving

Improving can only happen when you have measures, and measures can only be possible by tracking the success of your AI implementations. Begin by establishing clear, simple metrics for every AI use case deployed in your organization. C-suite leaders must resist their own bias toward wanting to see elaborate technical dashboards. Instead, focus on business outcomes that matter, such as time savings, employee satisfaction, error reduction, operational efficiency, and cost efficiency.

Adopt the concept of a Minimum Viable Measurement Dashboard (MVD), which is a streamlined approach that tracks only the key metrics needed to quickly validate a product or strategy. Its purpose is to prevent information overload, highlight early insights, and guide rapid improvements based on essential user feedback and business indicators. The MVD acts as a template that standardizes which metrics are tracked, why, and how data is collected.

The following is a sample MVD (for illustrative purposes only):

Metric	Why It Is Important	How to Capture
Use Case Adoption Rate	Reveals utilization and user buy-in	Collect via system logs and surveys
Time Savings	Indicates efficiency gains	Compare before/after processing times
Error/Override Rate	Uncovers quality concerns	Sample manual reviews and system flags
Staff Feedback Score	Measures satisfaction	Anonymized surveys, NPS scores
ROI Estimate	Links impact to financial outcomes	Pair time saved with average hourly costs

Firms can consider adopting measures such as:

- **AI Document Intake.** Monitor how many documents are processed automatically, average time per document, and reduction in manual errors.
- **Chatbots and Email Triage.** Track the percentage of inquiries resolved without human intervention, average response times, and feedback from users.
- **Underwriting Support.** Measure time saved per case, accuracy in flagging unusual applications, and frequency of manual overrides.
- **Claims Automation.** Record cycle time reduction, changes in customer Net Promoter Score (NPS), and audit error rates.
- **Generative AI.** Gauge staff satisfaction, the number of tasks completed, and the quality of responses.

Scaling Surgically

It is critical to be precise and exact in which specific use cases you select and scale out. Only expand proven solutions that deliver value and are supported by users and stakeholders. Before scaling any AI use case, complete a simple checklist like the following:

- There is demonstrated positive impact (measured by metrics above).
- Employee adoption is stable or growing.
- There are no unresolved compliance or risk issues.
- Clear training materials are available.
- Internal champions are in place to support broader adoption.
- Monitoring dashboards are set up and regularly reviewed.

AI use case rollouts and scale outs should take a phased approach. Stagger and stage these rollouts by starting with a pilot phase, gathering robust and actionable feedback, and adjusting as needed. Communicate changes clearly to all involved, provide post-launch support, and designate points of contact from your internal AI Governance Committee for trouble-shooting. Scaling AI is not a one-time event, and you must create habits and behaviors that support ongoing improvement.

Below are some considerations that support a continuous improvement mindset:

- Hold regular reflection meetings to review what is working, what is not working, and reprioritize use cases.
- Set use case sunset criteria to shelve those that are falling short of expectations. For instance, reduce your use case "clutter" by taking a product life cycle perspective, shelving use cases with low usage or poor ROI. Those should trigger a pause or sunset.

- Participate in peer benchmarking studies and learning from similar carriers.
- Institutionalize a feedback mechanism for employees to provide feedback to the AI Committee and/or their direct leaders.
- Schedule regular vendor knowledge sharing sessions to stay informed about new features and best practices they are incorporating into their product roadmaps.
- Document every step, adjustment, and lesson learned. Build a living playbook that guides new deployments and upgrades, so that each future AI use case benefits from those that came before. Use checklists and templates for measurement, rollout, and review so the process is predictable, transparent, and easy to follow.

Scaling and continuous improvement are not just about adding more technology. They are about learning, measuring, and refining what works for your business. The C-suite leaders who take a disciplined, transparent, and adaptive approach will build an AI strategy that grows with their organization and delivers results year after year.

4.0 In Closing

Our industry is experiencing a transformative shift driven by advancements in AI and GenAI. This evolution not only enhances existing processes, but it also reshapes the insurance landscape. By leveraging AI strategically, insurers can achieve significant competitive advantages, drive innovation, and better serve a new generation of customers. However, the rapid pace of AI evolution also presents new risk management challenges, particularly for small to midsize carriers that must balance modernization with resource constraints.

This playbook seeks to provide a pragmatic approach for small to midsize carriers to adopt AI responsibly. Your firm should emphasize the importance of selectively deploying intelligent AI solutions to address critical issues, streamline routine tasks, and enable teams to perform more effectively. Grounded in insights from LIMRA and LOMA, this playbook has presented a step-by-step roadmap tailored for small to midsize carriers, focusing on practical considerations, business value, and regulatory compliance.

By following this framework, carriers can implement AI solutions without extensive investments in infrastructure or specialized teams, while maintaining sound oversight and governance practices. The goal is to empower leadership to realize the advantages of AI, enhance internal expertise, and build confidence in AI-driven transformations. This structured approach ensures that AI adoption remains sustainable and evolves with organizational needs, ultimately helping to close the protection gap and deliver affordable protection to underserved communities.

Adopting and scaling AI in a smaller insurance company does not require a team of in-house data scientists or sophisticated technical resources. Instead, leaders should focus on developing a blended talent approach — one that combines upskilling existing employees, engaging trusted external partners, and empowering business leaders to take ownership of AI initiatives. This strategy ensures flexibility, reduces cost, and embeds AI into the company's core operations.

Key Principles

- **You do not need a dedicated AI team.** The goal is to cultivate AI-literate decision-makers within your organization by means of leaders, product owners, and analysts who can collaborate with vendors and consultants to drive meaningful results. Create a cross-functional AI Committee within your firm.
- **Upskill the willing.** Prioritize AI training for those who show enthusiasm, curiosity, and motivation. These individuals bridge the gap between business needs and technical possibilities. You do not need to create AI engineers, but you must develop an AI-literate workforce.
- **Strategically outsource.** When specialized expertise is needed, use outside talent, consultants, or vendor services. This enables your company to access high-level skills without long-term hiring commitments.
- **Empower middle management.** Domain experts and subject matter experts should co-own AI projects with external partners, ensuring solutions are relevant and sustainable.

Actionable Steps

1. **Identify AI Champions**

- Conduct a short survey or open call for volunteers interested in AI.
- Assign "AI champion" roles to those who express interest and have the domain knowledge to influence processes. This person ensures requirements are clear and aligned with company objectives.
- Provide AI champions with dedicated training resources and invite them to vendor demos and pilot projects.

2. **Build a Hybrid Team Structure**

- **AI Strategy Lead:** Appoint an outside CIO, CTO, or an external advisor to guide AI priorities, vendor selection, and project oversight.
- **Data Steward:** Appoint and potentially upskill a business analyst within each business unit to bridge data, business goals, and technical solutions.
- **Compliance Point Person:** Pair your existing compliance personnel with part-time AI legal support to oversee regulatory and ethical obligations.
- **Business Owner:** Select a domain expert or subject matter expert who understands your business processes and cross-domain workflows, and who can evaluate AI output for practical relevance.
- **External AI Partner:** Contract with vendors or consultants for modeling, integration, and experimentation. Use retainer or project-based agreements to control costs.

3. **Focus on Upskilling**

- Choose user-friendly AI platforms and tools such as those already available to most firms (for example, Microsoft Copilot, ChatGPT, and Google) to lower technical barriers to entry.
- Set up regular learning sessions featuring case studies, vendor walkthroughs, and AI basics.
- Encourage self-paced online learning through resources.
- Incentivize skill development with gamification, recognition programs, certificates, or small bonuses for those who complete AI training modules.

4. **Leverage External Partnerships**

- Tap into industry governance groups and leverage the resources available. Adopt industry standards, frameworks, and best practices. Leverage the insights to educate yourselves and your teams.
- Engage regional academic institutions for access to interns, research, and shared resources.

- Contract with outside CIOs/CTOs or independent advisors for strategic planning, vendor evaluation, and oversight.
- Work with vendors or offshore teams to clean and prepare data, enabling rapid experimentation and scaling.
- Retain legal or regulatory AI external counsel for policy development and compliance reviews.

5. Emphasize Governance and Change Management

- Form an internal AI Governance group comprised of business unit leaders, IT, compliance, and other functions to oversee project selection, risk management, and progress tracking.
- Make change management a deliberate part of the process. Be intentional, communicate frequently, celebrate quick wins, and address change resistance through transparent Q&A sessions and hands-on demos.
- Ensure all training and project plans align with company culture, regulatory requirements, and strategic goals.

Ultimately, AI is not a replacement for human intelligence, but a powerful tool that, when used responsibly, can amplify our capabilities and drive transformative change. In the age of AI, the key to success lies not in the technology itself, but in the strategic vision and human ingenuity that guide its implementation. The path to AI-driven transformation is paved with collaboration, continuous improvement, and a steadfast commitment to leveraging technology for the greater good.

Advancing the financial services industry by empowering our members with

LIMRA LOMA
Navigate With Confidence

0931-2025