1. Consider Adoption of its 2025 Fall National Meeting Minutes

Attachment One

Commissioner Michael Yaworsky (FL)

Draft: 12/17/25

Innovation, Cybersecurity, and Technology (H) Committee
Hollywood, Florida
December 11, 2025

The Innovation, Cybersecurity, and Technology (H) Committee met in Hollywood, FL, Dec. 11, 2025. The following Committee members participated: Michael Yaworsky, Chair (FL); Angela L. Nelson, Co-Vice Chair (MO); Mark Fowler (AL); Michael Conway represented by Jason Lapham (CO); Doug Ommen (IA); Marie Grant (MD); Mike Chaney represented by Ryan Blakeney (MS); James E. Brown (MT); Jon Godfread represented by John Arnold and Colton Schulz (ND); Judith L. French (OH); Mike Humphreys represented by Diana Sherman (PA); and Elizabeth Kelleher Dwyer (RI). Also participating were: Lori Dreaver Munn (AZ); Sandra Darby (ME); Christian Citarella (NH); Cassie Brown (TX); Scott A. White and Michael Peterson (VA); and Rosemary Raszka (VT).

1. Adopted its Nov. 17 and Summer National Meeting Minutes

The Committee conducted an e-vote that concluded Nov. 19 to adopt its 2026 proposed charges.

Director Nelson made a motion, seconded by Commissioner Fowler, to adopt the Committee's Nov. 17 (Attachment One) and Aug. 13 minutes (*see NAIC Proceedings – Summer 2025, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. Adopted the Reports of its Working Groups and Subgroup

   A. Big Data and Artificial Intelligence (H) Working Group

Commissioner Ommen stated that the Working Group met Nov. 19 and requested additional redline feedback on the *Artificial Intelligence (AI) Systems Evaluation Tool* by Dec. 2. He said the Working Group received comments from interested regulators and parties. These comments were summarized into a comparison chart for discussion. Commissioner Ommen stated that during its meeting at the Fall National Meeting, the Working Group discussed the detailed feedback received on the background, intent, and scope of the *AI Systems Evaluation Tool*. The Working Group also discussed comments from interested parties concerning Exhibit A, with the goal of finalizing the edits for the next version of the Tool.

The Working Group's agenda also planned for discussion of edits and comments on Exhibit B, Exhibit C, and Exhibit D of the tool. However, due to the robust discussion, the Working Group was unable to discuss those exhibits during the meeting.

Edits discussed during the meeting ranged from minor refinements to the specific wording and phrasings to more substantial and conceptual feedback and concerns, including how the Tool would be administered in the context of a market conduct or financial condition examination, the confidentiality protections, and whether and how the Tool would be coordinated with a lead regulator. The Working Group also discussed whether the Tool should only be focused on high-risk AI models with direct impact, how to assess and measure the extent of the usage of AI System models by an insurer, whether to include all insurer operations in scope, and whether to include certain types of AI model algorithms.

The Working Group also discussed the pilot process for the Tool and heard comments suggesting that the Working Group develop a pilot planning document that would describe the pilot's parameters.

After evaluating the discussion during this meeting and incorporating the edits, Commissioner Ommen stated that he expects that a third draft of the Tool, along with a comment chart with the issues the Working Group was unable to discuss, may be taken up at an additional interim Working Group meeting. Working Group members suggested that the Working Group could discuss Exhibit B, Exhibit C, and Exhibit D at an interim meeting.

Once the Working Group has completed the revisions, it is expected that the Tool will be piloted by a few state departments of insurance (DOIs) in 2026 to gather feedback on their experiences administering the Tool. During this time, the Working Group will continue to coordinate with the Market Regulation and Consumer Affairs (D) Committee and Financial Condition (E) Committee, as well as other working groups and task forces. At the conclusion of the pilot period, the Working Group will revise the Tool based on the experience gained from the pilot process and may re-expose it. At that point, the Working Group may revisit its discussion on next steps.

B. Cybersecurity (H) Working Group

Peterson next gave an update on the Cybersecurity (H) Working Group's activities. He stated that the Working Group has convened on several occasions since the Summer National Meeting.

Peterson reported that the Working Group met at the Fall National Meeting, where it heard comments on the *Cybersecurity Event Notification Portal* project intake form. The Working Group's work centered on achieving convergence in the implementation and operation of the *Insurance Data Security Model Law* (Model #668), aiming to reduce marginal compliance costs for insurers and streamline regulatory processes. The portal project proposal was posted for comment before the meeting, and the Working Group addressed feedback received during this meeting.

Peterson also provided the Committee with a summary of the portal proposal, which would provide a single, unified platform for receiving and managing notifications. Once the Working Group adopts its proposal, it anticipates seeking approval from the Committee and later presenting the proposal to the Executive (EX) Committee. Yaworsky stated that the project will result in a platform that will add value to the work of the regulators.

The Working Group also met Sept. 30 in regulator-to-regulator session, pursuant to paragraph 4 (internal or administrative matters of the NAIC or any NAIC member) of the NAIC Policy on Open Meetings, to receive an update on the Working Group's ongoing work to discuss the development of the Cybersecurity Event Notification Portal.

Additionally, the Working Group met Sept. 25 and took the following action: 1) discussed and received comments on the insurance data security model (IDSM) compliance guide, which was designed to help state DOIs enforce compliance with Model #668 more effectively, and the Chief Financial Regulator Forum referral response; and 2) adopted the compliance guide.

C. Data Call Study Group

Schulz provided an update on the Data Call Study Group's ongoing activities. He stated that the Study Group continued its work to create an inventory of data elements collected by the NAIC and regulators, along with their definitions. The Study Group shifted its focus from statutory financial statement data to market data and data element definitions. NAIC staff finalized lists of data elements and definitions for the homeowners data call and Market Conduct Annual Statement (MCAS) datasets, and edited and validated an initial data scrape of NAIC statistical data available to regulators.

The Study Group chair monitored activities and met periodically with lead regulators of various market data efforts. The Study Group aimed to finalize a master list of market data elements and definitions, supplementing it with elements from recent state-specific data calls. Once complete, the Study Group plans to meet in regulator-to-regulator session to compare existing data elements to regulator needs and identify gaps.

After gap identification, industry representatives from key insurers and trade associations would be invited to review the regulators' list of data element gaps and provide comments. The Study Group would then finalize its list of needed data elements and definitions, moving toward operationalizing data collection. The overarching goal was to reduce the number of ad hoc data call requests by different states, promote consistency, and improve the quality and timeliness of regulatory data.

D. Third-Party Data and Models (H) Working Group

Lapham gave an update on the work of the Third-Party Data and Models (H) Working Group. He stated that the Working Group met during the Fall National Meeting. During this meeting, the Working Group adopted minutes from previous meetings and discussed the exposure of a draft third-party data and model regulatory framework. The framework, developed by a subgroup of regulators from Colorado, Florida, Iowa, Pennsylvania, and Vermont, was released for a 60-day exposure period ending Feb. 6 to solicit written comments from interested parties.

The draft framework applies to property/casualty (P/C), health, and life insurance, requiring third-party vendors to register with state insurance departments if their data or models are used in insurer functions with direct consumer impact. The framework provided confidentiality and trade secret protections for third parties, similar to those afforded to insurers, and outlined a discretionary filing process for receiving data or models.

The framework's goals are to ensure regulators have timely access to third-party data and models and to confirm that vendors maintain strong governance practices. It covered insurance functions, such as pricing, underwriting, claims, utilization reviews, marketing, and fraud detection. Governance standards for models included documentation of purpose, assumptions, inputs, limitations, performance metrics, and validation processes. For data, standards included accuracy, completeness, timeliness, representativeness, auditability, lineage, and quality controls.

Lapham said the Working Group emphasized that insurers remained fully responsible for compliance with all applicable laws and regulations.

E. SupTech/GovTech (H) Subgroup

Munn provided an update on the SupTech/GovTech (H) Subgroup's activities. She stated that the Subgroup met Dec. 2 in regulator-to-regulator session, pursuant to paragraph 6 [consultations with NAIC staff] of the NAIC Policy Statement on Open Meetings. During this meeting, NAIC staff presented on Compliance Language Assistance for Regulatory Analysis (Clara), an AI-powered tool designed to assist regulators in reviewing rate and form filings more efficiently. The demonstration highlighted Clara's "human in the loop" approach, showing how the tool flags potential compliance issues while ensuring that regulators retain full decision-making authority.

The session also provided information about the states participating in a pilot program for Clara and offered insight into the tool's development roadmap. The Subgroup expressed interest in evaluating future presentations and educational opportunities for 2026 and invited fellow regulators to suggest topics that would benefit collective understanding and oversight capabilities.

Munn invited regulators to reach out to Subgroup leadership or NAIC staff with suggestions for future topics and emphasized the Subgroup's commitment to ongoing education and technological advancement in regulatory practices.

Director Nelson made a motion, seconded by Director Dwyer, to adopt the reports of the: Big Data and Artificial Intelligence (H) Working Group, including its Nov. 19 and Sept. 29 minutes (Attachment Two); Cybersecurity (H) Working Group, including its Sept. 25 minutes (Attachment Three); Data Call Study Group; Third-Party Data and Models (H) Working Group, including its Oct. 19 and Sept. 26 minutes (Attachment Four); and SupTech/GovTech (H) Working Group. The motion passed unanimously.

3. Adopted the Privacy Protections (H) Working Group Report and Request for NAIC Model Law Extension

Director Dwyer gave an update on the Privacy Protection (H) Working Group's activities. She stated that the Working Group met Dec. 3 in regulator-to-regulator session, pursuant to paragraph 6 (consultations with NAIC staff members related to NAIC technical guidance) of the NAIC Policy Statement on Open Meetings, to discuss next steps for drafting and Article VI. She said that she anticipated releasing revised Article VI, without comment, soon.

The Working Group also met Nov. 7 in open session and heard comments on Article VI, Exceptions to Limits on Disclosures of Nonpublic Personal Information.

Additionally, the Working Group met Sept. 22 in regulator-to-regulator session, pursuant to paragraph 6 (consultations with NAIC staff members related to NAIC technical guidance) of the NAIC Policy Statement on Open Meetings, to discuss next steps for drafting and Article V, Limits on Disclosures of Nonpublic Personal Information, of the *Privacy of Consumer Financial and Health Information Regulation* (#672), which includes, among others, sections on the sale of nonpublic personal information and limits on the disclosure of sensitive personal information. As a result of this meeting, as well as the drafting group's Aug. 1 open session, the Working Group released revised Article V. The revised Article V can be found on the Privacy Protections (H) Working Group's website under the exposures tab. Comments are not being requested on Article V at this time. There will be a public comment period following the next exposure of the complete revised draft of Model #672.

Director Dwyer stated that, in lieu of meeting at the Fall National Meeting, the drafting group continues to make progress revising Model #672 section by section and will continue to hold open and regulator-only meetings as needed. She said that the drafting group will submit the full revised draft of Model #672 to the full Working Group for consideration and exposure once the section-by-section review is complete.

Director Dwyer made a motion, seconded by Commissioner Ommen, to adopt the Working Group's report and grant the Working Group's request for an extension of time until the 2026 Fall National Meeting to continue drafting the revised Model #672. The motion passed unanimously.

4. Heard a Presentation from Conning on AI in Insurance

Manu Mazumdar (Conning) began by introducing Conning as an insurance asset management company with a long history and a dedicated insurance research group. Mazumdar explained that Conning conducted an annual survey of C-suite executives in the insurance industry to assess the adoption and impact of AI and related technologies.

Mazumdar traced the evolution of AI, noting its roots in the 1940s and its growing influence in the insurance sector. He emphasized that AI is no longer an emerging technology but has become integral to the insurance business value chain, from underwriting and claims to client engagement. The 2025 survey revealed a dramatic shift: 90% of respondents were in some stage of implementing generative AI, with 55% in early or full adoption—a nearly 100% increase year-over-year. Full adoption of large language models surged from 18% to 63% in just one year, and machine learning (ML) and predictive analytics have reached 74% adoption.

Mazumdar detailed how AI adoption varied across business functions. In sales and underwriting, generative AI, large language models, and ML tools have seen widespread adoption, with similar trends in operations and claims. He highlighted that the insurance workforce was evolving, with significant growth in higher-skilled, higher-paid roles, such as data science and actuarial positions, while administrative roles have declined. Mazumdar projected that future workforce skills would need to blend technological fluency, critical thinking, creativity, adaptability, and regulatory proficiency.

He concluded that AI is driving efficiencies, reducing costs, and enabling hyper-personalized customer experiences. However, he stressed the importance of balancing innovation with empathy, governance, and trust, and noted that the human element would remain essential in both developing and utilizing AI systems.

Commissioner Yaworsky asked Mazumdar about the AI winter referenced in the presentation, which took place in the 1980s, and whether there were any lessons to be drawn from that. Commissioner Yaworsky then inquired about where the greatest growth in AI use might occur within insurance operations—whether in underwriting, customer interaction, claims, or back-office functions. Mazumdar replied that growth was occurring across the board. He provided an example of how AI tools were enhancing both operational efficiency and customer interactions, such as enabling staff from various departments to handle customer calls more effectively during catastrophe events by leveraging AI-driven support.

Commissioner Yaworsky asked whether ML continues to play a role in shaping innovation. Mazumdar said that all the technologies will remain relevant, but that he views the discussion as a sort of building block situation, where some AI plays a foundational role and other, more advanced techniques like generative AI would likely play an overarching role.

Director Nelson remarked that she appreciated the discussion in Mazumdar's presentation about the continued reliance on human involvement. She asked how much of the innovation Conning is observing relates to back-office or more consumer-facing interactions. Mazumdar responded that the P/C industry was primarily focused on operational efficiency, while the life industry was adopting technologies such as wearables. However, he explained that each sector had its own nuanced approach to technology adoption. Mazumdar added that he also expected to see innovation across the board, for instance, in underwriting or other operational areas. He noted an example where, in responding to a natural catastrophe, companies are using AI to help receive information from policyholders and help augment staff capabilities with informational resources to assist in the support being provided.

Having no further discussion, the Innovation, Cybersecurity, and Technology (H) Committee adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2025_Fall/WG-BDAI/Fall-Minutes/H-Minutes121125.docx

2. Consider Adoption of the Reports of its Working Groups and Subgroup

A. Big Data and Artificial Intelligence (H) Working Group
B. Cybersecurity (H) Working Group
C. Privacy Protections (H) Working Group
D. Third-Party Data and Model (H) Working Group
E. SupTech/GovTech (H) Subgroup

Attachment Two

Commissioner Michael Yaworsky (FL)

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

3. Receive an Update on the Cybersecurity Event Notification Portal

Attachment Three

Commissioner Michael Yaworsky (FL) and Michael Peterson (VA)

Please check all that apply:	
State Connected	☐
Operational	☐
Regulator Request	☒
Urgent Request *(Requires Immediate EPMO review)*	☐

Name of the Project/Initiative:	Centralized Cybersecurity Event Notification Portal Project
Project Sponsor(s):	Michael Peterson
Person Completing Proposal:	Koty Henry
Submission Date:	03/13/2025

1. **OPPORTUNITY STATEMENT: When answering this question, please describe:**
   - *Why do we need to implement this project?*
   - *What problem are we trying to solve for?*
   - *How do we know this IS a problem to solve for?*
   - *Have we ever done something like this before?*

The current cybersecurity event notification process required by the Insurance Data Security Model Law #668 (MDL #668) is fragmented and inconsistent across the jurisdictions where it has been passed, adopted, and implemented. This is burdensome for licensees to navigate during a cybersecurity event, adding significant costs to an already expensive process, and increases legal risk due to inconsistent compliance expectations. Additionally, this complexity is a friction point for the industry as legislatures consider the adoption of MDL #668, as licensees must bear additional compliance requirements. Lastly, the Cybersecurity (H) Working Group has charges that would be imperiled by inaction or failure, particularly charges #3 and #8. Without the additional efficiency a central portal would create, developing guidance for cyber events and coordinating any resulting work (Charge #3) would remain overly complicated and slow. Finally, assisting with the passage and implementation of MDL #668 (Charge #8) cannot be reasonably achieved so long as the marginal cost of compliance with a jurisdiction's notification requirement remains high, a problem the central portal will address. In summary, as cybersecurity risks intensify, this lack of a unified, efficient reporting system hinders timely response, complicates compliance, and weakens stakeholder confidence.

The Cybersecurity (H) Working Group has been working to align the various areas of MDL #668 and the centralized cybersecurity event notification portal is the final piece. Already, guidance documents have been adopted to reduce the compliance burden of industry by aligning the efforts of departments of insurance as they enforce sections 6 and 7: the Cybersecurity Event Response Plan (CERP), and the Insurance Data Security Model Law Compliance and Enforcement Guide. While both have been adopted and address necessary areas of convergence, the ability to

centralize the reporting of cybersecurity events requires technology, not a guide. This project is that technology.

The basic technology underlying the portal, being able to store and receive highly sensitive information while limiting access to only the appropriate users and aligning with well recognized control frameworks and will include clear governance over security, requirements well within the NAIC's capabilities and expertise. This initiative aligns with the CERP adopted in March 2024 and supports the implementation of MDL #668.

2. **PROPOSED SOLUTION: When answering this question, please describe:**
   - *What is the proposed or "ideal" solution?*
   - *What are the intended outcomes?*
   - *Are there any "Hard" Dates to consider?*
   - *Are there any known risks to account for?*

The Cybersecurity (H) Working Group adopted the CERP on March 17, 2024, which guides state insurance regulators on responding to cybersecurity event notifications, required under Section 6 of MDL #668, from licensees. The CERP, however, can only unify the response to a notification by departments, not the underlying requirements faced by licensees to provide notification in the first place. The proposed solution is to develop a secure, centralized portal hosted by the NAIC to receive, manage, and track cybersecurity event notifications from licensed entities in states that have adopted MDL #668.

The portal would be built with a minimum of features, aiming for a high degree of uniformity within a licensee-directed notification system. To accomplish this, a set of notification questions that represent the requirements of all MDL #668 states will be developed into a single, standardized notification form (attachment 1). Data access will be highly limited to only those departments with an adopted version of MDL #668, and the responsibility for selecting those departments will be upon the licensee. Additionally, security concerns should be assuaged by an annual disclosure of a System and Organization Controls Reporting (SOC) 3 report by the NAIC. The SOC 3 report is the public version of the NAIC's SOC 2 Type II that is conducted annually, and their report looks at the Security Trust Services Criteria.

Lastly, as we develop experience additional opportunities may present themselves wherein the portal may be improved. Any such future endeavor will be done in consultation with our stakeholders and interested parties.

Key Features

- Licensee fills out a single, standard notification form, which may be updated as additional facts become known. A draft version of the standard form can be found in attachment 1, where additional details about uploading files can be found.
- Licensee directs notifications by selecting the departments to notify, which may be updated. Secure, role-based access for regulators, providing access only for those who have passed an equivalent to Section 6 of MDL #668.

- Regulators to have the ability to satisfy recordkeeping requirements by downloading completed records.

3. **KEY RESOURCES: When answering this question, please describe:**
   - *What resources/teams are required to deliver the solution?*
   - *What is the projected resource level of estimates for each affected area?*

   The success of a centralized cybersecurity event notification portal relies on the collaboration of internal NAIC teams and regulators, in particular the Cybersecurity (H) Working Group, as well as collaboration with licensees, as warranted.

   Resource needs for this initiative have been identified as follows:
   - *NAIC technical and cybersecurity teams for development and hosting*
   - *Regulatory and legal input to align with state law variations*
   - *Business analysts and project managers to oversee implementation*
   - *Training and support staff for successful rollout and adoption*
   - *Infrastructure Investment (servers/cloud services, licences)*

4. **EXISTING ALTERNATIVES: When answering this question, please describe:**
   - *Do we have an in-house solution in place that COULD meet the existing need?*
   - *Is a new purchase/build absolutely required to meet the project needs?*

   While no single solution currently provides this fully tailored experience, the NAIC has tools and platforms that can enable an efficient and scalable build of such a solution.

5. **VALUE PROPOSITION: When answering this question, please describe:**
   - *Why should the organization invest in this initiative?*
   - *What value will be created by doing this?*
   - *What happens if we DON'T do this?*
   - *If applicable, please indicate the letter committee that adopted this project.*

   The portal is the final piece of a series of initiatives intended to harmonize and align the various cybersecurity requirements found in MDL #668. Once complete, the NAIC membership should be able to more easily pass MDL #668 nationwide, as legislatures will face fewer hurdles from industry as their problems with the law's expansion will have been solved. Further, the streamlined compliance and improved incident response that licensees will achieve will improve operational efficiency by reducing compliance costs and complexity. The portal will allow licensees the ability to submit information about cybersecurity incidents once within the security of the NAIC's systems rather than to multiple states, multiple times, through multiple platforms containing varying levels of security.

   Many issues will arise if this project is not pursued. Without a central solution there will continue to be duplicative regulatory efforts to investigate cybersecurity breaches and varying levels of security for submission of cybersecurity breach notifications across departments. Most importantly, failing to align requirements will make it difficult for MDL #668 to be passed in

additional jurisdictions, imperiling work on the Cybersecurity (H) Working Group's Charges #3 and #8.

6. **KEY SUCCESS METRICS: When answering this question, please describe:**
   - *What key deliverables will make this project a success?*
   - *How will we know when we are successful?*
   - *What key metrics will be used to define "Doneness"?*
   - *How will we test/validate metrics?*

   The key deliverables necessary to make this project a success would include developing a portal that:
   1. Meets both industry and regulator confidence requirements regarding data security and confidentiality.
   2. Allows licensees to submit cybersecurity event notifications through the portal to those jurisdictions that have adopted a version of Section 6 of MDL #668 that licensees determine should be notified.
   3. Allows each state regulator to receive all information necessary to meet the statutory reporting requirements of their jurisdiction via a standard form.
   4. Allows both regulators and industry participants to satisfy their recordkeeping requirements through secure downloads and robust logging to ensure auditability.
   5. Allows licensees to update the information within the notification, via the portal, as their investigation progresses.
   6. Notifies licensee-selected regulators via email when new information is available for viewing.
   7. Allows licensees to update which regulators who have adopted MDL #668 have access to the cybersecurity event notification, in keeping with their legal responsibilities.

   To measure the success of the proposed centralized portal for cybersecurity event notifications, the following key metrics may be considered:
   1. Number of Cybersecurity Event Notifications: Track the total number of notifications received through the portal to assess adoption and usage.
   2. User Adoption Rate: Monitor the number of licensees and state insurance regulators using the portal and the growth rate of new users. *Maybe consider quantifying the metric by saying something like "**Adoption by at least 5 states in Year 1; goal to scale to 10+ within 2 years**"*
   3. User Satisfaction and Feedback: Collect and analyze feedback from users through incremental surveys to measure satisfaction, system uptime, and identify areas for improvement.

7. **CUSTOMER SEGMENTS: When answering this question, please describe:**
   - *What is the impact to the organization, members, another project or NIPR if this project is not approved?*
   - *Who is the customer/member? Who is your audience?*
   - *Who are the business owners/stakeholders that will be impacted by this?*

- *Who are the end users?*

Without a central solution there will continue to be duplicative regulatory efforts to investigate cybersecurity breaches and varying levels of security for the submission of cybersecurity breach notifications across departments. Most importantly, failing to align requirements will make it difficult for MDL #668 to be passed in additional jurisdictions, imperiling work on the Cybersecurity (H) Working Group's Charges #3 and #8.

The key stakeholders for this project are members and licensees. Departments of insurance whose legislature has passed a version of Section 6 of MDL #668 will have access to a central repository where every cybersecurity event notification they are legally entitled to is available. This will reduce work for departments as they review and track individual notifications and reduce duplicative and redundant responses. Further, for those states whose legislature has not passed a version of MDL #668 but would like to, the centralized portal will reduce the regulatory burden experienced by licensees as more states adopt.

Licensees will accrue the immediate benefit of a centralized repository as the burden for notifying multiple state departments of insurance will be dramatically reduced through the implementation of a standard form and a push-based, licensee-directed system. Currently, licensees must navigate multiple regulatory schemes for the notification of cybersecurity events, all with their own unique approaches to implementation. This fragmentation has led to a slow and ultimately expensive process for licensees.

8. **COST STRUCTURE: When answering this question, please describe:**
   - *What known costs are associated with the project (i.e., Software, Hardware costs, etc.)*
   - *Are there any 3rd party vendor costs to consider?*

Staffing Options & Estimate:

Below are Assumptions and Staffing Options/Estimates for the Centralized Cybersecurity Event Notification Portal Project EPMO proposal dated 2/11/26. Note that the timing of this effort could affect the quoted amounts and timelines based on staff availability.

Assumptions:

- Deliverable will be a single solution for all jurisdictions.
- Prototype using Appian and Design review with Working Group is completed prior to project approval by EPMO.
- Team is comprised of Product Owner, 3 Software Engineers and 1 Software Quality Engineer
- Prototype is for discussion purposes; the team will meet UI/UX and Appian guidance for the development work.
- Option one assumes the team is working 75% of the time on this project with the rest of the time allocated to other work to support existing applications.

The following phases are recommended:

Phase	Key Activities
Project Preparation Phase	Training (Option 2), planning, understanding project, refinement of work.
Development (MVP)	Build core features: intake form, role-based access (admin, company and regulator, audit trail, notifications). Reuse components and tables from UCAA and SERFF where appropriate.
Testing & Validation	Functional testing, automation testing, Dynatrace Synthetic, security validation, UAT with early adopters.
Pilot Rollout (5–10 states)	Controlled launch, feedback loop, refinements.
Full Rollout & Support Setup	Training, documentation, help desk, onboarding additional states.

- H Committee staff support will provide ongoing administrative support.
- On-going staff considerations also include .25 ITG FTE for maintenance and support post-release.

Staffing Options/Estimates

1. **A dedicated ITG delivery team with existing Appian development experience and no outside help.** This team will not need startup and training time/costs; however, this option may not be feasible based on anticipated workloads.

Cost: $0 consulting costs – NAIC internal labor only
Duration: 7.5-8 months

2. **An ITG delivery team with no Appian development experience and the assistance of one full-time NAIC Appian Software Engineer.** This approach enables the delivery team to complete current tasks within an extended duration. Training and startup time allocated is included for a team new to Appian. The mentor's team will have reduced capacity for the duration of the project.

Cost: $16,500 instructor led training and certification for 3 engineers, the team will be unavailable for other work.
Duration: 9.5-10 months

3. **Outsourced to a professional services consulting group, with oversight of NAIC staff.**

Cost: $2.1M consulting costs, and reduced capacity of NAIC staff working with outside firm
Duration: 7.5-8 months

9. **RISK MITIGATION: What risks should you mitigate to make the project successful? When answering this question, please describe known risk factors associated with implementing this**

project, such as:

- *Are there risks to achieving a high adoption?*
- *Is this a new effort we've never done before?*
- *Do we need to acquire innovative technology to implement?*

The NAIC is exceptionally well positioned to construct and administer the portal, and it fits well into its existing expertise. Accepting data, even highly sensitive and confidential data, is something NAIC does well and has done for a long time across many domains. However, some general risks remain, which are discussed below.

Risk: Stakeholders lack a method by which to understand the current security posture of the portal.

Mitigation: NAIC should make available, annually, a SOC 3 report for public review by licensees and other interested parties. The SOC 3 is the public version of a SOC 2, an industry-recognized and respected third-party assurance report, which preserves the sensitive security information of the NAIC.

Risk: Access and confidentiality protections for licensees.

Mitigation: Access to the portal will be based on whether a department's legislature has passed a version of Section 6 of MDL #668. The licensee, utilizing a push-based system, will select the departments to receive their notification as their legal responsibility requires. Like the form, the departments able to view the notification can be updated by the licensee. The NAIC will have limited access to enable support only, and will mirror the access they retain for other, highly sensitive information like RBC data, ORSA reports, and exam information.

Risk: Difficulty in tracking changes and updates to a notification by departments.

Mitigation: Given the simplicity of the design of the portal, with licensee-directed notifications, this difficulty is best addressed through a robust logging capability. This will provide the necessary insight for departments to understand how the notification has been changed and updated over time.

Risk: The underlying data increases in its sensitivity, which may result in higher cybersecurity risk to the licensee cybersecurity event information.

Mitigation: If highly sensitive information begins to be included in the portal, then cybersecurity risk becomes elevated in importance. To handle the prospective risk of elevated cybersecurity, a SOC3 report should be provided annually, which will ensure stakeholder clarity that highly sensitive information is adequately secured by NAIC.

Risk: Using the portal is difficult and causes problems for departments.

Mitigation: Clear instructions will be made available and training, if necessary, will be developed and offered.

While other risks may be present, all the risks found insofar have been found to have mitigation strategies that are acceptable to stakeholders.

10. **Member Support:** When answering this question, please document the members who are in support of this initiative.

Ensuring the alignment of the majority of members is crucial for the success of any initiative. The new EPMO project process is structured to foster collaboration and build consensus through a transparent, phased approach:

- The proposal will first be presented to the Cybersecurity (H) Working Group, providing a focused forum for subject matter experts and key stakeholders to evaluate the initiative, raise concerns, and offer recommendations. This early engagement ensures technical and operational considerations are addressed before moving forward.
- Following the Working Group's input, the proposal will advance to the Innovation, Cybersecurity, and Technology (H) Committee for broader member review. This step allows for strategic alignment across the organization to ensure that all members have an opportunity to provide feedback and influence the direction of the project.

This transparent, consensus-focused approach will provide the necessary alignment among all stakeholders to allow for member support to build organically.

11. **PROJECT DEPENDENCIES: Is this project dependent on other projects or initiatives? If yes, please list.**

No, this project does not depend on other projects or initiatives.

12. **HARD DEADLINES: Is there a deadline driving this project? ☐YES ☒NO If yes, what is it?**

13. **REVENUE STREAMS/SOURCES:** **When answering this question, please describe:**

- **Will this effort generate additional revenue or cost money to implement? ☐YES ☒NO**

Revenue generation from non-licensees may be explored in later phases. The current proposal is not predicated upon the recovery of costs from licensees.

- **If so, what is the revenue projection?**

14. **Could an additional fee be charged to recoup costs and/or are there future budgetary cost**

savings? ☐YES ☒NO

15. Will NIPR share costs? ☐YES ☒ NO If yes, indicate your rationale and list the NIPR contact.

16. Provide high-level estimates for the initial and future costs associated with this project.

- **Please insert additional rows if needed.**

Software Licenses and/or Subscriptions – Type *(include maintenance on separate line)*	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term	% Allocated to NIPR
				3-Year	
		$			
TOTAL		$			

Hardware Purchases – Type *(include maintenance on separate line)*	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term *(maintenance only)*	% Allocated to NIPR
		$			
		$			
TOTAL		$			

Consulting – Staff Aug. Position Title (each requested consultant on its own line)	Proposed Hourly Rate or Fixed Engagement	Estimated Hours for Contract Term	Length of Contract Term	Starting Month and Year	% Allocated to NIPR
	$				
	$				
TOTAL	$				

Consulting – Prof. Services Position Title (each requested consultant on its own line)	Proposed Hourly Rate or Fixed Engagement	Estimated Hours for Contract Term	Length of Contract Term	Starting Month and Year	% Allocated to NIPR
TOTAL					

Training / Conferences / Certifications - Type	Number Requested	Individual Cost	Month and Year Attending or Start of Subscription	Is this an annual subscription. (Yes / No)	% Allocated to NIPR
		$			
		$			
TOTAL		$			

Travel – Purpose and Location if Known	Number Individuals Traveling	Number of Nights per Individual	Individual Cost from Current Travel Matrix	Month and Year of Travel
			$	
			$	
TOTAL			$	

New Headcount Requests – Job Description Title	Number Requested	Proposed Salary	Starting Month and Year
		$	
		$	
TOTAL		$	

17. What assumptions have been factored into the project estimates?

- It is assumed that the number of workforce identities will remain consistent at 1,000 over the 3-year term. While this number is currently accurate, the NAIC may experience growth.
- The estimates assume that the implementation and integration of the Identity and Access Management (IAM) tool with existing systems (Active Directory, Okta, eDirectory, Workday) will be completed within the planned timeline without significant delays.
- It is assumed that internal teams, including the IAM team and identity teams, will be available and have the necessary expertise to support the implementation and integration efforts.
- The estimates assume that the selected IAM tool will be compatible with the NAIC's existing identity systems and will not require significant additional customization or development.
- The cost estimates do not include a managed service offering for ongoing support. The NAIC may choose to purchase this offering in the future.

18. Please indicate the staff resources needed for this project in the table below.

Please insert additional rows if needed. Only technical hours will be tracked for the project.

Replace 0 with numbers. Highlight Total Number, Right click, Update field.

Internal Resources	Area/Team	Number/Type (Ex: 2-Analysts, 3-SE)	Total Estimated Hours

19. What is your confidence level in the above estimates? ***Low estimates will not be considered by the EPMO*****.**

☐ **HIGH**
Please comment:

☐ **MEDIUM**
Please comment:

20. Does the project include any of the following: PII/MNPI/other confidential information, attachments or ad-hoc data access? ☐**YES** ☐**NO**
If yes, please provide details regarding the confidential information, size, and number of attachments/retention period or ad-hoc data access needs.

-
-
-
-

For EPMO use only – do not fill out.

Account Description	Account Code / Dept	Total Expense for Initial Budget Year	Estimated Expenses for Following Year	Total Capital for Item (if Applicable)	Starting Month of Amortization or Depreciation	Length of Term	% Allocated to NIPR
		$	$	$			
		$	$	$			
Totals for EPMO spreadsheet		**$**	**$**	**$**			
Totals for NAIC		**$**	**$**	**$**			
Totals for NIPR		**$**	**$**	**$**			

3. Hear a Presentation on Insurance Artificial Intelligence (AI) Trends, Including Agentic AI Applications

Attachment Four

Scott Froseth, Ilana Golbin Blumenfeld, and David Sherwood (PricewaterhouseCoopers)

Insurance AI Trends, Including Agentic AI Applications

A PwC Perspective for NAIC

PwC

March 2026

With you today

Scott Froseth
Partner
P&C Insurance Operations

Ilana Golbin Blumenfeld
Partner
Tech & Data - Responsible AI Lead

Eras of Insurance Technology of Manual Effort

Reduced Human Effort:

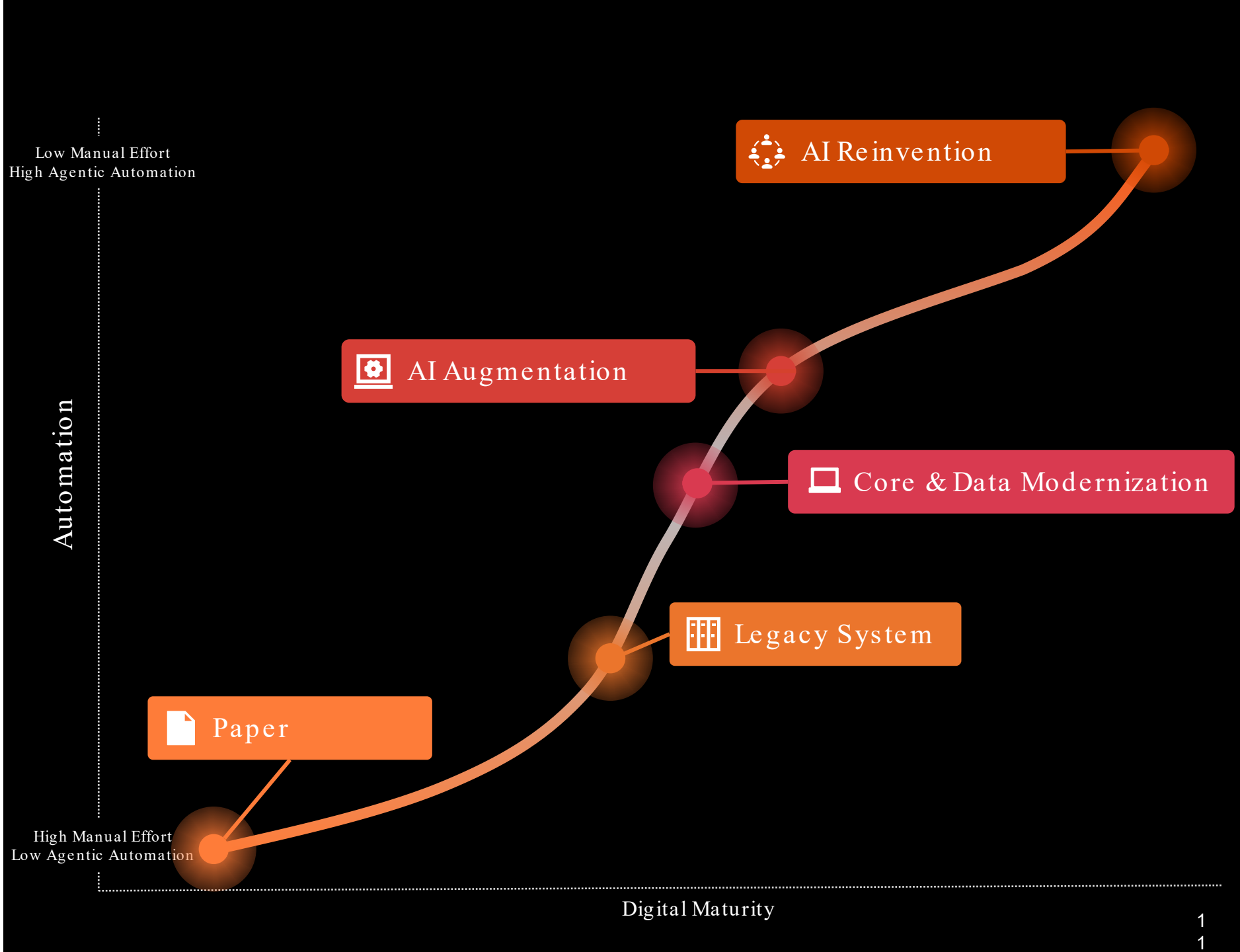
Each era reduces manual effort through advancements in technology

Progressive Innovation:

New systems build on the foundations of previous platforms and processes

AI Frontier:

The next phase explores pushing boundaries with AI beyond core transformations, using AI to completely transform functions



Defining the modern AI Agent

The term “AI Agent” is widely used in the media and corporate setting, but definitions vary widely and are often too narrow or incorrect - the following effective definition sets the context for our discussion

GenAI	
What it does	Produces content (text, images, code, etc.) from user prompts
Common use cases	• Drafting emails or documents • Answering questions • Brainstorming ideas • Writing summaries or reports

Agents	
What they do	Act on your behalf to complete tasks, make decisions, and manage workflows across systems
Common use cases	• Processing support tickets • Automating refund approvals • Scheduling meetings • Automating lead qualification

GenAI helps generate content...Agents get things done

Their **autonomy**, **intentionality**, and **adaptive learning** push them well beyond deterministic automation—turning static processes into self-optimizing systems

What makes up an AI Agent?

Knowledge

Agents draw on knowledge to provide context-aware support

Tools & Actions

Agents can run tools, like navigating product screens or editing files

Context Memory

Agents retains knowledge across conversations

Interaction Models

Users can interact with Agents through voice and text channels

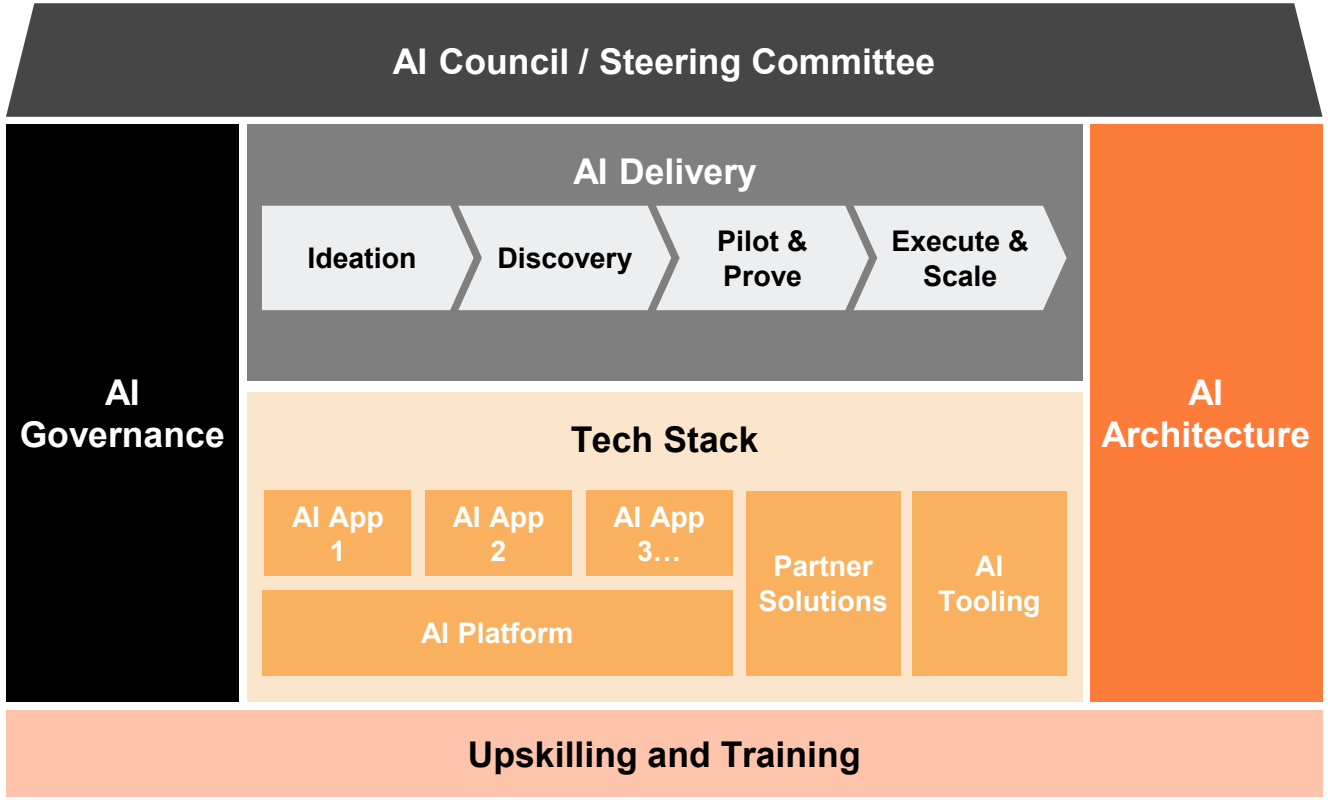
Workflows

Agents understands the user’s intent to run the correct workflows

The building blocks of the AI Operating Model for AI enablement

Aligning these core AI operating model components to the organization's structure and maturity, emphasizing the areas most critical to effective implementation and scale.

Operating Model Key Components



Overview

The interactions and dynamics between these components will vary based on the selected structure and maturity, but each plays a critical role in an effective AI strategy:

- **AI Council / Steering Committee:** Responsible for overall AI Strategy direction, key decisions, escalations, and funding
- **AI Governance:** Responsible for safeguarding key information, managing risk, and facilitating compliance
- **AI Delivery:** Main driver for use case implementation and driving business value
- **Tech Stack:** Foundational technology components and applications to facilitate solution
- **Architecture:** Responsible for defining the architectural guiding principles and standards are met when developing AI use cases
- **Upskilling & Training:** Responsible for upskilling resources across all teams as well as conducting change management activities

Personalization: An AI operating model that reflects ways of working, embeds practical governance, and accelerates adoption across key business functions.

AI is already becoming a disruptive force in commercial insurance

Carriers are moving fast to reinvent the industry, embracing emerging technologies to modernize operations, launch digital offerings, and redefine customer experiences*

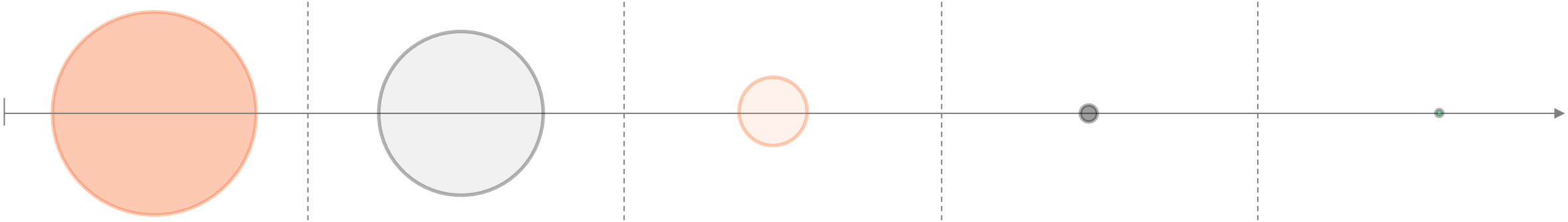
Carrier	Story	Impact
MARKEL Insurance Business, Mar 12, 2026	Markel International launches an **AI Center of Enablement** and appoints its **first Head of AI** to accelerate responsible AI deployment across five global insurance businesses	Enables **scalable AI deployment** across global operations to improve broker, employee and client outcomes
CHUBB Chubb, Nov 12, 2025	Chubb Launches **AI-Powered Embedded Insurance Engine** to Personalize Digital Partnerships	**Strong customer value proposition** and rapid growth through AI-native distribution
ZURICH *Zurich, July 9, 2025*	Over 1,000 Zurich employees across 40+ countries developed **200+ working prototypes** in 4 weeks	Saves **~60 minutes per underwriting submission** through AI-generated narratives
AIG Reinsurance News, Nov 7, 2025	AIG deploys AI solution that **ingests broker submissions** and extracts structured data to **accelerate commercial underwriting**	**Improves submit-to-bind** ratios and **underwriting speed**, enabling AIG to process rising commercial submissions at scale
THE HARTFORD CIR Magazine, Aug 6, 2025	The Hartford deployed a Gen AI solution to **automatically classify submissions** and extract key data from unstructured underwriting documents	Reduced average processing time by about **20 minutes per case**, enabling underwriters to focus on higher value tasks
TRAVELERS Travelers, Feb 18, 2026	Travelers launches an **agentic AI Claim Assistant,** developed with **OpenAI**, to handle customer claim intake through intelligent voice conversations	Enhances FNOL **customer experience** and **accelerates claim initiation** while enabling claims teams to focus on resolution
Nationwide Nationwide, Oct 29, 2025	Nationwide commits **$1.5B in technology investment through 2028**, including **$100M annually to scale AI** across underwriting, claims and service workflows	Accelerates **advanced AI capabilities** through targeted funding
Allianz Allianz, Feb 18, 2025	AllianzGPT, an internal chat bot, combines the power of GenAI with **internal data integration**	Boosts employee productivity through **AI-enabled enterprise knowledge** access
Allstate	Allstate revealed almost **all of the communications** reps send out to claimants are written by AI	Noted AI communications are **more compassionate** than human generated

* Sourced from public information only

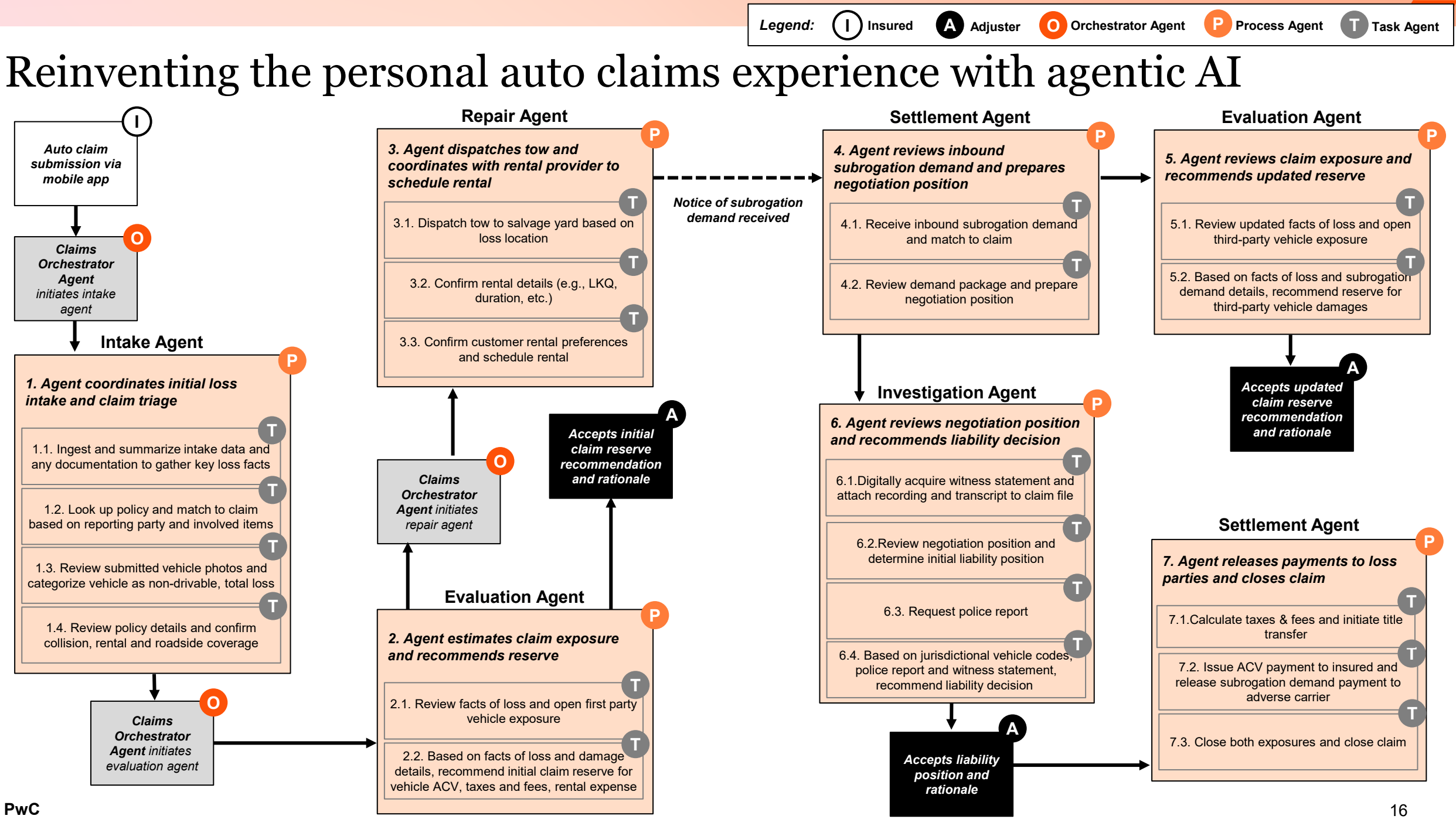
Insurance carriers are at different points of their AI maturity

1	2	3	4	5
Passive / Pull-Through	**Point Use Cases**	**Agentic Process**	**Operating Model Redesign**	**New Revenue Stream / Businesses**
Individual productivity gains with minimal or no process redesign	Targeted automation applied to specific steps inside the existing process	End-to-end redesign where AI agents orchestrate a defined segment; humans handle exceptions and oversight	Structural redesign of roles, governance, and capacity because the work itself has changed	Establish new products, services, and business models that generate net-new revenue beyond core operations
Speed to market	**Limited disruption**	**Reimagines workflow**	**Achieves scale**	**Creates new revenue streams**
Scale to many users	**Limited scale**	**Near-term efficiency gains**	**Maximizes long-term ROI**	**Monetizes data & AI capabilities**
Difficult to measure	**Easier change management**	**Compartmentalizes benefits**	**First mover advantage**	**Expands into new markets**

Market Maturity

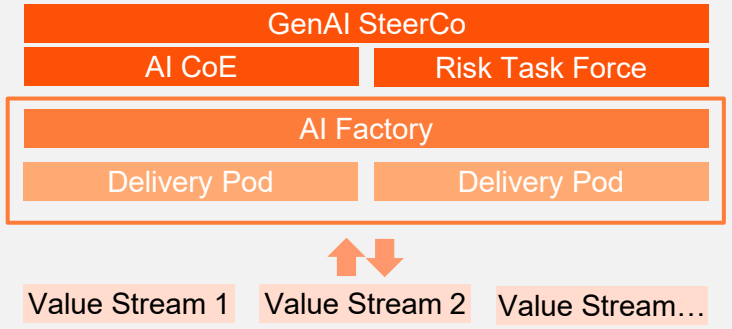


Size of bubble illustrates relative number of carriers leveraging approach


Legend:
Insured
Adjuster
Orchestrator Agent
Process Agent
Task Agent
Reinventing the personal auto claims experience with agentic AI
Auto claim submission via mobile app
Claims Orchestrator Agent initiates intake agent
Intake Agent
1. Agent coordinates initial loss intake and claim triage
1.1. Ingest and summarize intake data and any documentation to gather key loss facts
1.2. Look up policy and match to claim based on reporting party and involved items
1.3. Review submitted vehicle photos and categorize vehicle as non-drivable, total loss
1.4. Review policy details and confirm collision, rental and roadside coverage
Claims Orchestrator Agent initiates evaluation agent
Evaluation Agent
2. Agent estimates claim exposure and recommends reserve
2.1. Review facts of loss and open first party vehicle exposure
2.2. Based on facts of loss and damage details, recommend initial claim reserve for vehicle ACV, taxes and fees, rental expense
Accepts initial claim reserve recommendation and rationale
Claims Orchestrator Agent initiates repair agent
Repair Agent
3. Agent dispatches tow and coordinates with rental provider to schedule rental
3.1. Dispatch tow to salvage yard based on loss location
3.2. Confirm rental details (e.g., LKQ, duration, etc.)
3.3. Confirm customer rental preferences and schedule rental
Notice of subrogation demand received
Settlement Agent
4. Agent reviews inbound subrogation demand and prepares negotiation position
4.1. Receive inbound subrogation demand and match to claim
4.2. Review demand package and prepare negotiation position
Evaluation Agent
5. Agent reviews claim exposure and recommends updated reserve
5.1. Review updated facts of loss and open third-party vehicle exposure
5.2. Based on facts of loss and subrogation demand details, recommend reserve for third-party vehicle damages
Accepts updated claim reserve recommendation and rationale
Investigation Agent
6. Agent reviews negotiation position and recommends liability decision
6.1.Digitally acquire witness statement and attach recording and transcript to claim file
6.2.Review negotiation position and determine initial liability position
6.3. Request police report
6.4. Based on jurisdictional vehicle codes, police report and witness statement, recommend liability decision
Accepts liability position and rationale
Settlement Agent
7. Agent releases payments to loss parties and closes claim
7.1.Calculate taxes & fees and initiate title transfer
7.2. Issue ACV payment to insured and release subrogation demand payment to adverse carrier
7.3. Close both exposures and close claim

Across three observed models for driving AI transformation, clarity of roles and execution of desired model are as important as structure

Centralized Model

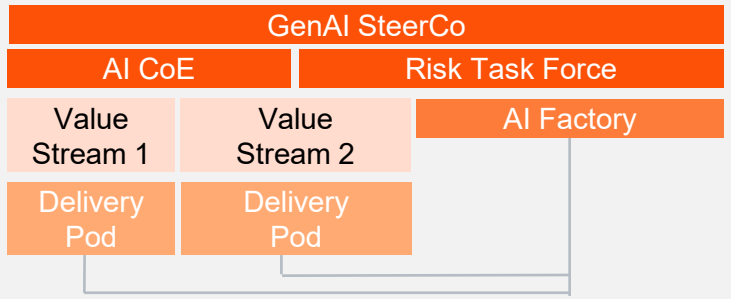


AI Council manages demand / prioritization and governance & oversight; **AI Factory** manages use case build & deployment and platform enablement.

Pros
- Lower cost, economies of scale
- Enterprise visibility
- Reusable assets – data, model patterns, platform

Cons
- Risk of AI efforts becoming academic, with lower adoption by functions
- AI resources may be over-utilized

Balanced (Hybrid) Model

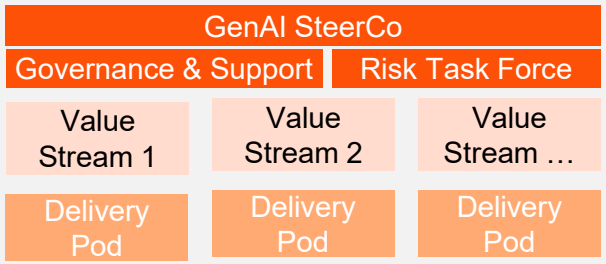


Functions jointly fund & are accountable; **AI Council** provides enablement & governance; Use case owners in hybrid pods work with **AI Factory** to build / deploy use cases

Pros
- Higher likelihood of adoption & accountability
- Data & Analytics Office to provide governance, standards & best-in-practice tools / talents

Cons
- Slightly higher cost with resources embedded to each business unit
- Potential for higher effort to ensure alignment across center & functional teams

Federated Model



Function leaders fund & are accountable, with support from IT; AI demand, build, and deployment managed by **individual functions**. Thin layer of governance oversight.

Pros
- Higher likelihood of adoption, with AI expertise embedded in each function
- Ability to build use cases for complex, domain-specific business needs

Cons
- Redundancy / duplication of work, higher cost
- Risk of minimal governance, RAI, privacy, lower likelihood of scale (PoC-itis)

Agent autonomy brings unmatched value…along with unignorable risks

Productivity Gains

- Frees up human talent for strategic work.
- Reduced operational overhead through automation.

Customer-Focused Personalization

- Hyper-personalized responses and experiences.
- Real-time adaptation to user behavior.
- Improved satisfaction and engagement.

Increased Scalability

- AI agents can synthesize vast amounts of data into actionable insights.
- AI agents can more easily tackle high volume, complex tasks across the organization.

Enterprise Resilience

- Reliable task execution can ensure business continuity.
- Reduces operational risk through consistent performance.
- Strengthens infrastructure against disruption.

01
02
03
04

01
02
03
04

Accountability Gaps

- Autonomous actions make it unclear who is responsible for outcomes.
- Overreliance can erode human expertise, especially in problem-solving.

Emergent Behavior

- Agents may develop unexpected strategies through interaction and adaptation.
- Outcomes can be non-deterministic, making them hard to predict or audit.
- Goal accomplishment may triumph regulatory or ethical boundaries, leading to novel behaviors.

Systemic Harm

- Cascading errors across multi-agent systems.
- Small bugs escalate into systemic breakdowns
- Reputational and regulatory consequences.

Infrastructure Gaps

- Existing infrastructure may not integrate well with agents.
- Scalability limitations can bottleneck performance.
- Lack of readiness for autonomous workflows.

AI Governance provide the guardrails that accelerate agentic innovation

AI and AI Agents proliferate across organizations through internal development, third party tools, and features embedded in productivity tools.

AI Governance can:

- Expedite responsible AI approvals to unlock opportunities and drive success
- Provides cross-functional alignment that enables innovation across the organization
- Proactively manage AI risks to stay ahead of potential disruptions
- Enable key stakeholders to anticipate change through governance-led feedback mechanisms
- Adapt proactively to shifting regulating and consumer demands
- Adhere to a set of standards/frameworks that enables defensible, transparent processes and decisions

Challenges organizations face in adapting AI program:

- Use-case-by-case AI governance assessments do not fit agentic systems
- Key decisions, approvals, and risk assessments miss context and change
- Lack of scalability of existing risk processes inhibit future progress
- Tool overload without strategy prevents an appropriate agentic ecosystem; third party risk is responsive to business asks and not designed to rationalize AI application procurement
- Limited stakeholder involvement leads to misaligned use goals
- Expanding userbase of AI applications stresses many existing governance programs given the wide range of understanding of BAU processes

Responding to the agent risks demands updates across the governance framework

Core Elements of a Responsible AI Framework

Foundational Capabilities

- AI Principles & Strategy
- AI Use Case Inventory 
- AI Risk Taxonomy 
- AI Risk Intake and Tiering 

Operating Model and Governance

- Operating Model - Roles & Responsibilities 
- Governance Committee and Escalations
- AI Risk and Control Matrix 
- Training and Communication 

Application Lifecycle

- AI Development and Deployment Standards 
- AI Testing and Monitoring 
- Risk Mitigation Tracking and Reporting 

Policies and Procedures Across Risk Domains (e.g., cyber, privacy, legal, model risk)

The gauge icons indicate components of the Responsible AI Framework that need to be updated when considering use of AI agents.

The level of updates can be low ( ), medium () or high ().

Dimensions of AI agent observability

The ability to explain AI systems by turning raw signals into evidence of why outcomes happen; making complex models, agent workflows, and emergent behaviors transparent, accountable, and controllable in real time.

Key Dimensions	Understanding AI Observability	Examples
System Behavior	**What is the AI doing and why is it making these decisions?**	• Prompt/response logs • Model decision traces • Agent workflows and chaining behavior
System Health	**Is the AI performing reliably and at the expected quality?**	• Latency and throughput • Error rates • Resource utilization (CPU, GPU, memory)
User Access	**Who is using the system, and how are they interacting with it?**	• Authentication and access logs • User roles and permissions • Session and usage activity
Data Flow	**What data is being used, where is it going, and what is produced?**	• Input/output lineage • Source access logs • Volume and frequency of data movement

Observability reveals what's happening inside AI systems; how they decide, perform and use data.

By collecting and connecting this evidence, organizations can spot risks early, reduce hallucinations, build trust, and utilize AI safely.

Q&A

Questions?