

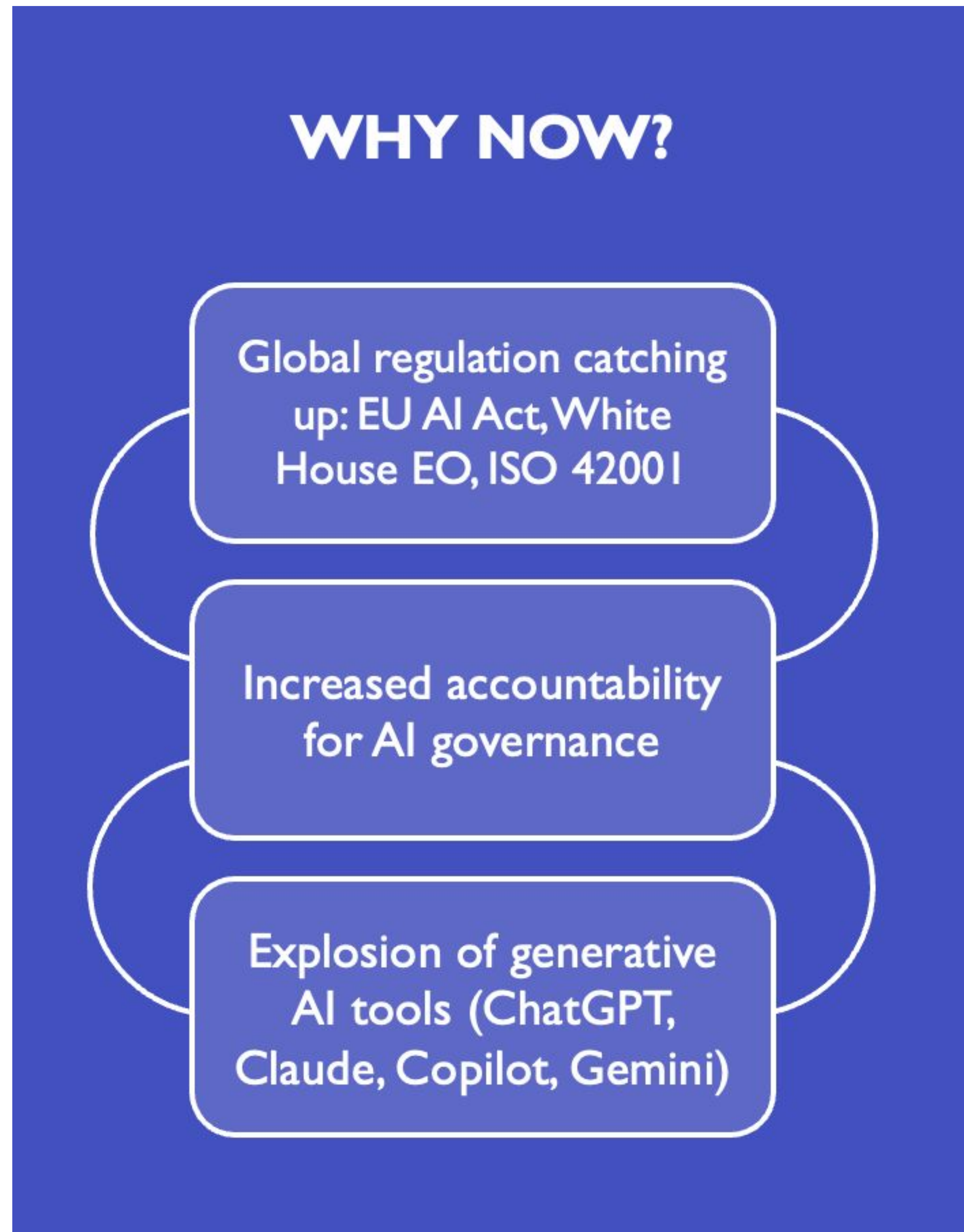
Complychain for *RegXperience**

Smart AI Risk Management for SMBs

[Abdul Khader](#) & [Divya Venkatraman](#)

& honorary member Dev Jadhav (who had proposed this project!)

AI Risk is Real..



AI Frameworks

Framework	Scope & Nature	Key Features	Compliance	Audience
NIST AI RMF Since Jan 2023	Voluntary, US-developed Risk-based	4 functions: Govern, Map, Measure, Manage Bias, robustness focus	Non-prescriptive Flexible	US orgs Risk adopters
ISO/IEC 42001 Since Dec 2023 <i>Only 16 organizations are certified</i>	International standard AI management systems	Structured governance Trust, terminology, documentation	Prescriptive Certifiable	Global orgs AI governance focus
OECD AI Principles Since May 2024	Non-binding Ethical guidelines	5 principles + 5 policy recs Human-centric approach	Advisory only No enforcement	Policymakers Strategy designers
EU AI Act Since July 2024	Legally binding Risk-based EU regulation	Tiered risk levels Strict for high-risk systems	Mandatory Penalties apply	EU-based AI deployers High-risk system devs
Singapore AI Verify Since May 2022	Voluntary, gov-developed Technical toolkit	Sandbox + tests Fairness, security, robustness	Voluntary Output-based reports	SG-based orgs Responsible AI pilots

Problem

Organizations are struggling to adopt AI governance!

Breaking down the problem - the **key challenges** in operationalizing AI Governance:

→ **Keeping Track of AI Systems:**

Organizations need a clear and up-to-date inventory of all their AI models and systems—what they are, where they're deployed, and who's responsible..

→ **Understanding What Rules Apply:**

They must stay informed about the latest AI risk regulations and frameworks to know exactly what rules and requirements apply to their systems.

→ **Proving Ongoing Compliance:**

They need a reliable way to regularly check if each AI system meets these requirements and to generate evidence of compliance when needed.

Our Solution

Key Challenges in Operationalizing AI Governance:

→ Keeping Track of AI Systems:

→ Understanding What Rules Apply:

→ Proving Ongoing Compliance:

Outcome Focus:

1. **Stakeholders: Independent**

Compliance consultants targeted on **SMBs** (limited resources, expertise, & budget to manage AI compliance)

2. **Reduce time** on compliance process

Iteration 1

ComplyAsset Agent

A workflow agent

Iteration 2

ComplyAsk Agent

A regulatory-aware RAG Agent

Iteration 3


ComplyAssess Agent



A human-in-the-loop workflow Agent

Design Specifics

Iterations	Cost/Latency	Optimizations	GuardRails	Eval Metrics
ComplyAsset Agent	Could be Rules-based system (with some LLM based for validation) for tracking + notifications.			
ComplyAsk Agent	VectorDB, Embedding LLM Calls	<ul style="list-style-type: none">- Search Bar- Restricted to copyrighted regulations- Only requirements will be vectorized	<ul style="list-style-type: none">- Relevance of Query term	<ul style="list-style-type: none">- Retrieval Accuracy (using labels from compliance managers)
ComplyAssess Agent	<ul style="list-style-type: none">- LLM Calls- Batch process not real-time assessment	Based on context length of evidence might require a RAG system	<ul style="list-style-type: none">- PII data masked before sending to LLM- Document Access Control	<ul style="list-style-type: none">- Judgement Consistency- Reasoning Hallucination- Accuracy vs human auditor judgement

Demo: RegXperience

 regxperience.tech

 **Welcome, Divya!**

Thanks for joining our early access program. You're among the first to explore how our platform simplifies compliance through automation and smart UX.


Here's what you can do today:

Ready for Review

These modules are live and ready for hands-on testing. Please explore their workflows, check how they align with your compliance needs, and share your feedback—your insights are critical to shaping the final product.

Work in Progress


These features are still under active development. You can hover over each icon below to see what's coming soon. If there are specific compliance workflows or tools you'd like to see added, let us know — we're building this with your needs in mind.

 **Your Feedback Matters**

Hit the "Share Your Feedback" button anytime to report issues, suggest improvements, or highlight what you love.


Share Your Feedback

COMPLIANCE TOOLS




REGULATIONS TO REQUIREMENTS

Upload any regulation. We will turn it into a clean list of actionable requirements—each one linked back to its source. Less reading, more doing.



REGULATORY MAPPING

Map those regulatory requirements to control frameworks like NIST, ISO, and more. See gaps, fix fast, stay ahead.



AI RISK MANAGEMENT

Assess AI systems against popular frameworks like NIST AI RMF and ISO 42001, enabling structured, standards-based risk evaluations.

ComplyAsk Agent

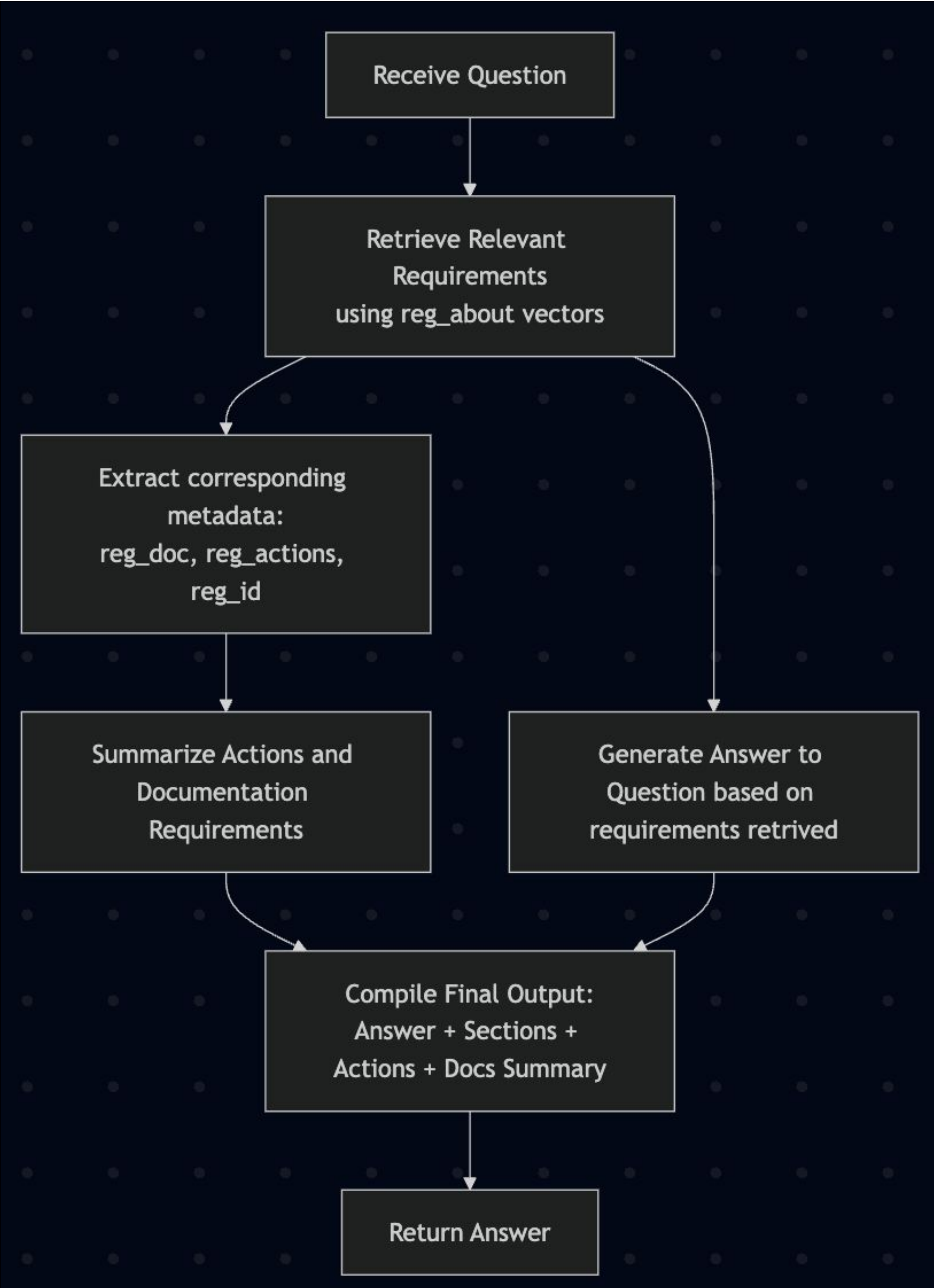
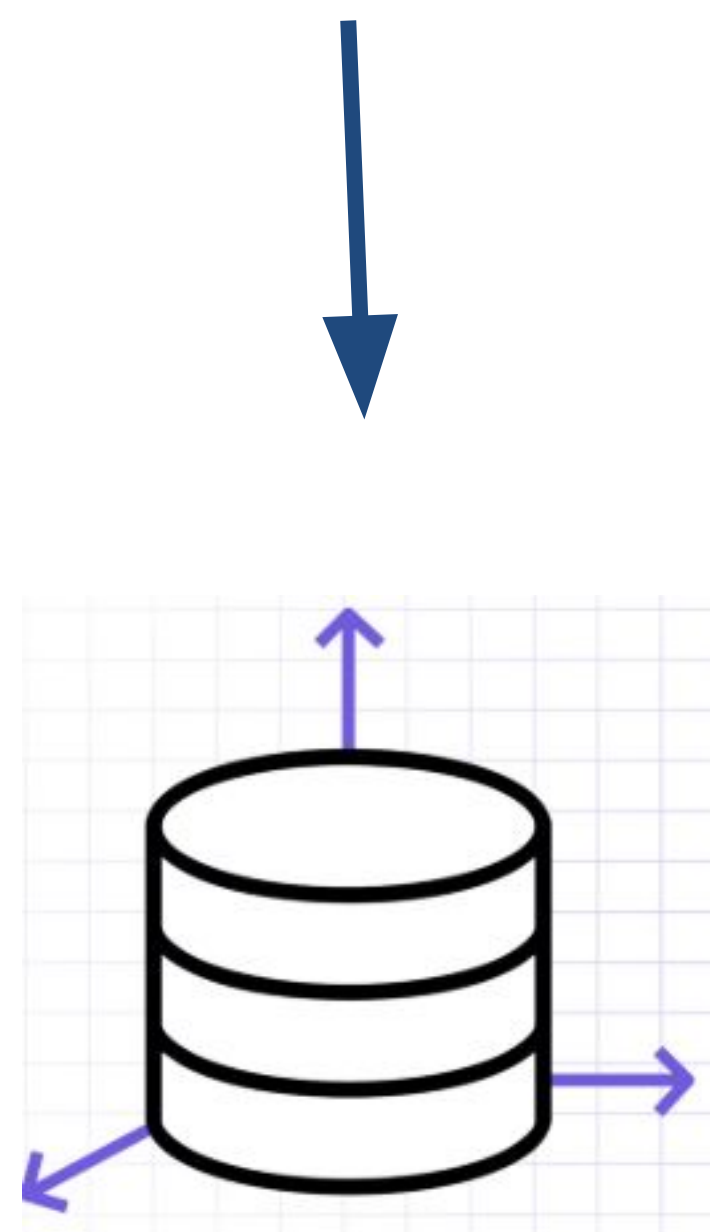
-> Search bar in AI RM(RegXperience)

<div><div>AllGovernManageMapMeasure</div><div><div>Search Controls</div><div>Find relevant controls with a question</div></div></div>		
Control	Description	
GOVERN 1.1	Legal and regulatory requirements involving AI are understood, managed, and documented.	i
GOVERN 1.2	The characteristics of trustworthy AI are integrated into organizational policies, processes, and procedures.	i
GOVERN 1.3	Processes and procedures are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	i
GOVERN 1.4	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	i
GOVERN 1.5	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned, organizational roles and responsibilities are clearly defined, including determining the frequency of periodic review.	i
GOVERN 1.6	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	i
GOVERN 1.7	Processes and procedures are in place for decommissioning and phasing out of AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	i

Mechanics: ComplyAsk Agent

NIST AI RMF

section_id	section_about	section_actions	section_doc	section_ref
GOVERN 1.1	<p>AI systems may be subject to specific applicable legal and regulatory requirements. Some legal requirements can mandate (e.g., nondiscrimination, data privacy and security controls) documentation, disclosure, and increased AI system transparency. These requirements are complex and may not be applicable or differ across applications and contexts.</p> <p>For example, AI system testing processes for bias measurement, such as disparate impact, are not applied uniformly within the legal context. Disparate impact is broadly defined as a facially neutral policy or practice that disproportionately harms a group based on a protected trait. Notably, some modeling algorithms or debiasing techniques that rely on demographic information, could also come into tension with legal prohibitions on disparate treatment (i.e., intentional discrimination).</p> <p>Additionally, some intended users of AI systems may not have consistent or reliable access to fundamental internet technologies (a phenomenon widely described as the “digital divide”) or may experience difficulties interacting with AI systems due to disabilities or impairments. Such factors may mean different communities experience bias or other negative impacts when trying to access AI systems. Failure to address such design issues may pose legal risks, for example in employment related activities affecting persons with disabilities.</p>	<p>* Maintain awareness of the applicable legal and regulatory considerations and requirements specific to industry, sector, and business purpose, as well as the application context of the deployed AI system.</p> <p>* Align risk management efforts with applicable legal standards.</p> <p>* Maintain policies for training (and re-training) organizational staff about necessary legal or regulatory considerations that may impact AI-related design, development and deployment activities.</p>	<p>### Organizations can document the following</p> <ul style="list-style-type: none">- To what extent has the entity defined and documented the regulatory environment—including minimum requirements in laws and regulations?- Has the system been reviewed for its compliance to applicable laws, regulations, standards, and guidance?- To what extent has the entity defined and documented the regulatory environment—including applicable requirements in laws and regulations?- Has the system been reviewed for its compliance to relevant applicable laws, regulations, standards, and guidance? <p>### AI Transparency Resources</p> <p>GAO-21-519SP: AI Accountability Framework for Federal Agencies & Other Entities. [URL](https://www.gao.gov/products/gao-21-519sp)</p>	<p>Andrew Smith, "Using Artificial Intelligence and Algorithms," FTC Business Blog (2020). [URL](https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms)</p> <p>Rebecca Kelly Slaughter, "Algorithms and Economic Justice," ISP Digital Future Whitepaper & YJoLT Special Publication (2021). [URL](https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf)</p> <p>Patrick Hall, Benjamin Cox, Steven Dickerson, Arjun Ravi Kannan, Raghu Kulkarni, and Nicholas Schmidt, "A United States fair lending perspective on machine learning," Frontiers in Artificial Intelligence 4 (2021). [URL](https://www.frontiersin.org/articles/10.3389/frai.2021.695301/full)</p> <p>AI Hiring Tools and the Law, Partnership on Employment & Accessible Technology (PEAT, peatworks.org). [URL](https://www.peatworks.org/ai-disability-inclusion-toolkit/ai-hiring-tools-and-the-law/)</p>



Results: ComplyAsk Agent

Question:

How are responsibilities for AI risk management assigned across teams and leadership?

Answer:

Responsibilities for AI risk management are assigned across teams and leadership by ensuring that senior leadership and members of

Relevant Section IDs:

['GOVERN 2.3', 'GOVERN 2.1']

Summary of Actions:

Key actions for AI governance and risk management include:

1. **Organizational Management**:

- Define and declare acceptable risk levels for AI systems.
- Actively support and engage in AI risk management.
- Cultivate a risk and harm prevention mindset throughout the AI lifecycle.
- Appoint and support qualified risk management leaders.
- Delegate authority and resources for risk management across the organization.

2. **Board and Committee Involvement**:

- Create board committees dedicated to AI risk management.
- Integrate AI risk management with broader enterprise risk strategies.

Summary of Documentation Requirements:

Internal teams focused on compliance, risk, and audit should document the following to demonstrate adherence to AI governance requirements:

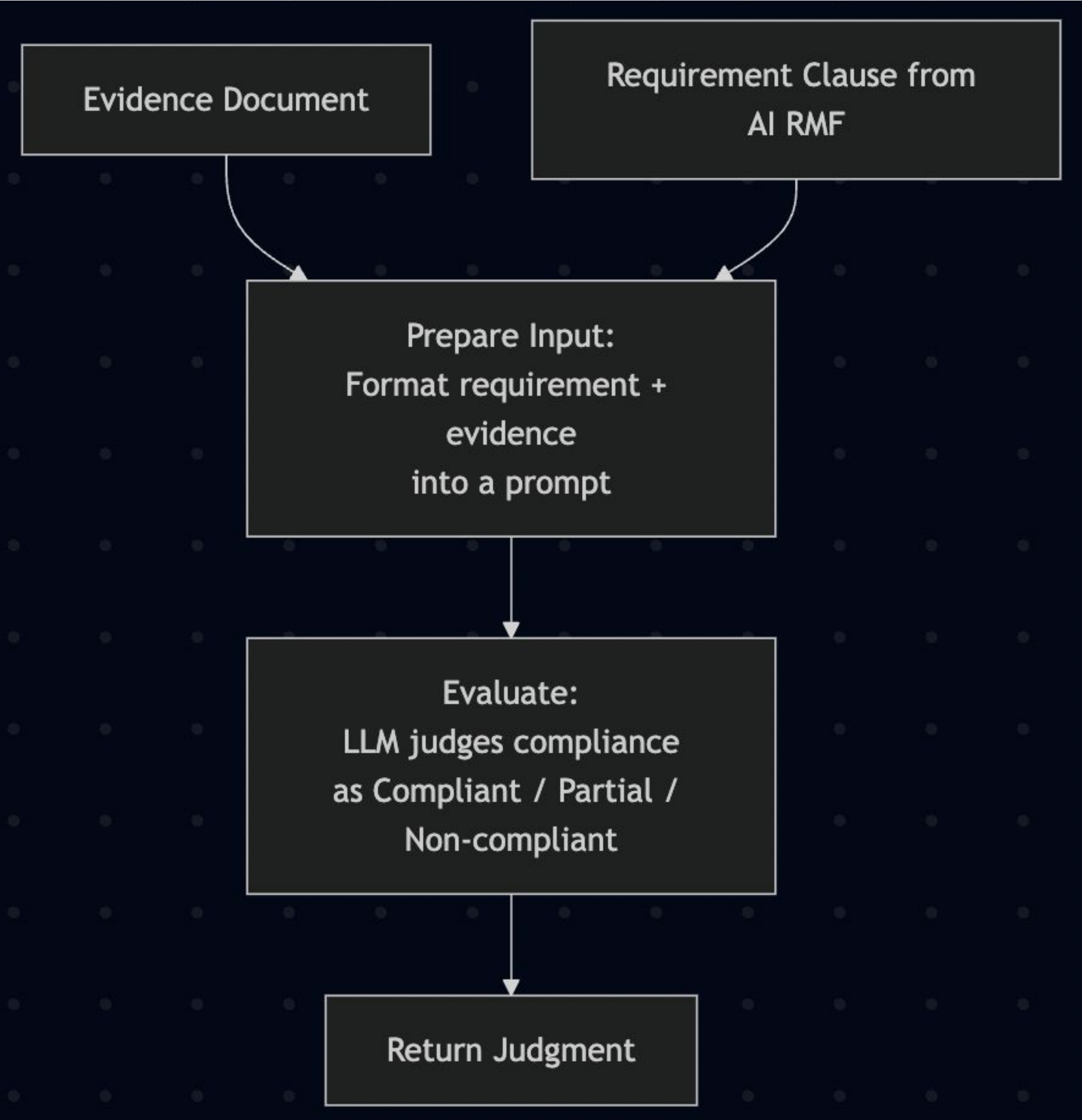
1. **Sponsorship and Participation**: Records showing that the organization's board and/or senior management sponsor, support, and participate in AI risk management.
2. **Roles and Responsibilities**: Clear documentation of the roles, responsibilities, and delegated authorities of personnel involved in AI risk management.
3. **Decision-Making Support**: Evidence that AI solutions provide adequate information for personnel to make informed decisions and take appropriate actions.
4. **Accountability Practices**: Documentation of practices related to accountability in data management and protection, ensuring alignment with organizational goals and regulatory requirements.

ComplyAssess Agent

-> Assess Button in AI RM(RegXperience)

GOVERN 1.5	<p>Ongoing monitoring and periodic review of the risk management process and its outcomes are planned, organizational roles and responsibilities are clearly defined, including determining the frequency of periodic review.</p>	<p>Established a "Risk Oversight Committee" comprising the CEO, Head of Product, and Lead Engineer. This committee meets monthly for the first 6 months post-launch, then quarterly thereafter, to review the AI RMF implementation status, assess new risks, review incident reports, and evaluate the effectiveness of mitigation strategies. The CEO is ultimately accountable for risk decisions.</p>	<p>Upload File</p>	<p>CALCULATED RISK</p> <p>Medium</p> <p>Impact High</p> <p>Likelihood Low</p>	<p>Not assigned</p>	<p>Mitigation Notes</p>
GOVERN 1.6	<p>Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.</p>	<p>Implementation Notes</p>	<p>Upload File</p>	<p>CALCULATED RISK</p> <p>N/A</p> <p>Impact</p> <p>Likelihood</p>	<p>Not assigned</p>	<p>Mitigation Notes</p>
GOVERN 1.7	<p>Processes and procedures are in place for decommissioning and phasing out of AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.</p>	<p>Implementation Notes</p>	<p>Upload File</p>	<p>CALCULATED RISK</p> <p>N/A</p> <p>Impact</p> <p>Likelihood</p>	<p>Not assigned</p>	<p>Mitigation Notes</p>

Mechanics: ComplyAssess Agent



Govern 1.6: An AI system inventory is an organized database of artifacts relating to an AI system or model. It may include system documentation, incident response plans, data dictionaries, links to implementation software or source code, names and contact information for relevant AI actors, or other information that may be helpful for model or system maintenance and incident response purposes. AI system inventories also enable a holistic view of organizational AI assets. A serviceable AI system inventory may allow for the quick resolution of:

- specific queries for single models, such as “when was this model last refreshed?”
- high-level queries across all models, such as, “how many models are currently deployed within our organization?” or “how many users are impacted by our models?”

AI system inventories are a common element of traditional model risk management approaches and can provide technical, business and risk management benefits. Typically inventories capture all organizational models or systems, as partial inventories may not provide the value of a full inventory.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
Model/System Name	Model Type	Deployment Status	Deployment Environment	Business Owner	Technical Owner	Training Data Source(s)	Data Dictionary / Schema	Documentation Link(s)	Source Code Repository	License / IP Info	Model Dependencies	Risk Classification	Use Case Category						
Credit Scoring Model	Classification	Deployed	GCP	Risk Management	Alice Tan	Internal banking datasets	https://bank.internal/docs/schema	https://bank.internal/docs/model_doc	https://git.bank.com/repo	Proprietary	scikit-learn, pandas	Medium	Loan risk assessment						
Fraud Detection AI	Anomaly Detection	In development	On-Prem	Fraud Division	John Lim	Internal banking datasets	https://bank.internal/docs/schema	https://bank.internal/docs/model_doc	https://git.bank.com/repo	Proprietary	scikit-learn, pandas	Medium	Fraud alerts						
Customer Churn Predictor	Regression	In development	Azure	Customer Retention	Sarah Lee	Internal banking datasets	https://bank.internal/docs/schema	https://bank.internal/docs/model_doc	https://git.bank.com/repo	Proprietary	scikit-learn, pandas	High	Retention offers						
Loan Approval Bot	Rule-Based NLP	Deployed	GCP	Lending	David Ong	Internal banking datasets	https://bank.internal/docs/schema	https://bank.internal/docs/model_doc	https://git.bank.com/repo	Proprietary	scikit-learn, pandas	Low	Loan eligibility						
Transaction Categorizer	Clustering	Deprecated	GCP	Finance	Meena Raj	Internal banking datasets	https://bank.internal/docs/schema	https://bank.internal/docs/model_doc	https://git.bank.com/repo	Proprietary	scikit-learn, pandas	High	Spending analysis						

Results: ComplyAssess Agent

ComplyAssess Agent: Judgment Details

Judgment:

Completely meets the requirement

Reasoning:

The provided evidence showcases an AI system inventory that is comprehensive and well-structured, meeting the governance requirement outlined. Here are the specific points supporting this conclusion:

Organized Database:

The inventory provides a detailed structure with columns such as Model/System Name, Model Type, Deployment Status, Deployment Environment, and more. This organizes relevant artifacts for each AI system effectively.

Essential Information:

It includes critical information like system documentation (Documentation Link(s)), incident response plans (Incident Response Plan Link), data dictionaries (Data Dictionary / Schema), and source code links (Source Code Repository). These are key elements mentioned in the governance requirement.

Contact Information:

Names and contact information for relevant AI actors (Business Owner, Technical Owner, Point(s) of Contact) are provided for streamlined communication.

Maintenance and Incident Response:

The inventory assists with model maintenance and incident response by including Date of Last Refresh, Initial Deployment Date, and Last Audit Date columns, which are crucial for tracking system updates and audits.

Holistic View and Resolution of Queries:

High-level metrics such as Model Version, Deployment Status, and Estimated Number of Users Impacted enable a holistic view. Queries like the number of deployed models or models' usage can be quickly resolved using this data.

Model Risk Management:

Risk Classification and AI Risk Control Measures columns align with traditional model risk management

Design Specifics

Iterations	Cost/Latency	Optimizations	GuardRails	Eval Metrics
ComplyAsset Agent	Could be Rules-based system (with some LLM based for validation) for tracking + notifications.			
ComplyAsk Agent	VectorDB, Embedding LLM Calls	<ul style="list-style-type: none">- Search Bar- Restricted to copyrighted regulations- Only requirements will be vectorized	<ul style="list-style-type: none">- Relevance of Query term	<ul style="list-style-type: none">- Retrieval Accuracy (using labels from compliance managers)
ComplyAssess Agent	<ul style="list-style-type: none">- LLM Calls- Batch process not real-time assessment	Based on context length of evidence might require a RAG system	<ul style="list-style-type: none">- PII data masked before sending to LLM- Document Access Control	<ul style="list-style-type: none">- Judgement Consistency- Reasoning Hallucination- Accuracy vs human auditor judgement