

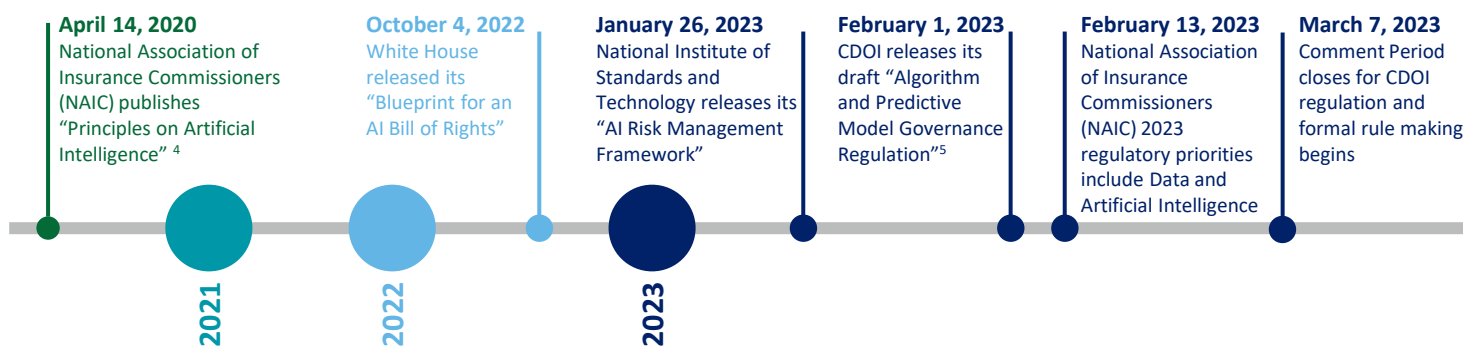
## Colorado Draft Artificial Intelligence (AI) regulation: Summary of governance and risk management framework (GRMF) requirements for life insurance companies

March 2023

## Overview of Colorado Division of Insurance’s (CDOI) draft AI regulation

The AI regulatory landscape continues to mature as government agencies refine and build upon previous guidance designed to manage AI risk, to reasonably ensure equality and transparency, and to provide trust in automated systems. This is evidenced by recent publications including the White House’s Blueprint for an AI Bill of Rights<sup>1</sup>, issued in October 2022, and the Artificial Intelligence Risk Management Framework<sup>2</sup>, issued by National Institute of Standards and Technology in January 2023. Additionally, the National Association of Insurance Commissioners (NAIC) continues to prioritize responsible data and AI use by insurers as reflected in its 2023 regulatory priorities<sup>3</sup>.

Figure 1 | Regulatory timeline



Continuing down the path of making the governance requirements more tangible, the CDOI, on February 1, 2023, issued its draft AI regulation intended to establish requirements for a life insurance company’s internal governance and risk management framework (GRMF) designed to reasonably ensure that life insurers’ use of external consumer data and information sources (ECDIS), algorithms, and predictive models (e.g., AI models) do not result in unfairly discriminatory insurance practices. This is believed to be the first such regulation on AI targeting insurers, and specifically life insurance. Based on recent regulatory trends, that other states may follow suit, and the scope may increase to other types of insurance (e.g., auto, property).

Figure 2 | CDOI AI regulation key terms

**Disproportionately negative outcome** means, for the purpose of this regulation, a result or effect that has been found to have a detrimental impact on a group as defined by race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, or gender expression, and that impact is material even after accounting for factors that define similarly situated consumers.

**External consumer data and information source or ECDIS** means, for the purposes of this regulation, a data or an information source that is used by a life insurer to supplement or supplant traditional underwriting factors or to establish lifestyle indicators that are used in insurance practices. This term includes credit scores, social media habits, purchasing habits, home ownership, educational attainment, licensures, civil judgments, court records, occupation that does not have a direct relationship to mortality, morbidity or longevity risk, and any insurance risk scores derived by the insurer or third-party from the above listed or similar data and/or information source.

## CDOI draft AI regulation requirements

### AI governance and risk management framework

Insurers dealing with life insurance are responsible to ensure that the following requirements are met, including instances where third-party vendors are engaged:

1. **AI governing principles** <sup>(5A1)</sup> to ensure that use of ECDIS and AI models using ECDIS do not lead to unfair discrimination
2. **Board & senior management oversight** <sup>(5A2)</sup> for setting and monitoring the overall strategy on the use of ECDIS and AI models and provide direction for AI governance
3. **Cross-functional governance committee** <sup>(5A3)</sup> with representatives from key functional areas
4. **Clearly assigned and documented roles and responsibilities** <sup>(5A4)</sup> of personnel involved with ECDIS and AI models
5. **Written policies and processes** <sup>(5A5)</sup> to ensure that ECDIS and AI models are documented, tested, and validated
6. **Training program** <sup>(5A6)</sup> for responsible and compliant use of ECDIS and AI models
7. **Controls** <sup>(5A7)</sup> to prevent unauthorized access to AI models
8. **Processes and protocols to address consumer complaints and inquiries** <sup>(5A8)</sup> about use of ECDIS and AI models
9. **Plan to respond to and recover from** <sup>(5A9)</sup> unintended consequences
10. **Engage outside experts for audits** <sup>(5A10)</sup> when internal resources are insufficient

### Minimum documentation

The below listed documentation must be regularly reviewed and updated to ensure accuracy and relevance and must be easily accessible to relevant personnel and available upon CDOI's request:

- i. **An inventory of ECDIS and AI models** <sup>(6A1)</sup> in use, with detailed descriptions, purpose, problem their use is intended to solve, potential risks, and safeguards
- ii. **Annual review of the inventory** <sup>(6A2)</sup> of ECDIS and AI models
- iii. **Tracking and managing changes** <sup>(6A3)</sup> to ECDIS and AI models, including version control
- iv. **Testing to detect unfair discrimination** <sup>(6A4)</sup> from use of ECDIS and AI models and steps taken to address disproportionate negative outcomes
- v. **Inputs** <sup>(6A5)</sup>, **outputs** <sup>(6A5)</sup>, **limitations** <sup>(6A6)</sup>, and **performance** <sup>(6A7)</sup> of AI models
- vi. Description of **dataset used to train** <sup>(6A8)</sup> **the AI models**, and how **predictions** <sup>(6A9)</sup> are made including any **assumptions** and **simplifications**
- vii. **Identification of potential risks** <sup>(6A10)</sup> (e.g., unintended bias) and impact on applicants, policyholders, and the insured
- viii. **Process of selecting external resources** <sup>(6A11)</sup> including third-party vendors
- ix. **Decisions made** <sup>(6A12)</sup> regarding use of ECDIS in the entire lifecycle of AI models

### Reporting

Once the final rule of the draft AI regulation goes into effect:

Insurers using ECDIS and AI models using ECDIS should submit the following –

- In **six months** <sup>(7A)</sup> following effective date of this regulation – A report summarizing progress toward complying with above mentioned requirements, areas under development, challenges encountered and expected completion date
- In **one year** <sup>(7B)</sup> following effective date of this regulation and **every two years thereafter** <sup>(7C)</sup> – A report demonstrating compliance with above requirements, along with supporting documentation

Insurers that do not use ECDIS and AI models using ECDIS should submit the following –

- In **one month** <sup>(7D)</sup> from effective date of this regulation and **annually thereafter** <sup>(7D)</sup> – An attestation indicating they do not use ECDIS

\*Note – the requirements above referenced (e.g., '5A1') refer to specific draft requirements of the CDOI draft AI regulation

## Deloitte’s Trustworthy AI™ Framework

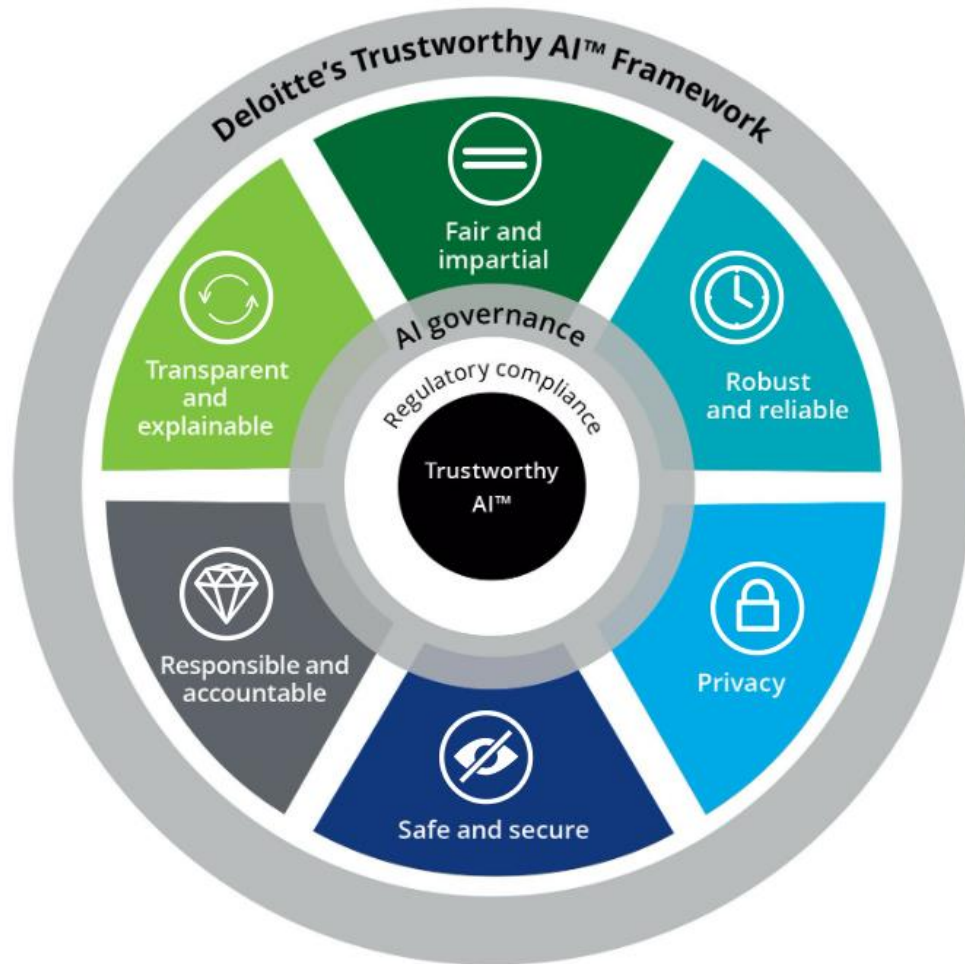
At Deloitte, we recognized the critical importance of the need for protections and for AI-Fueled organizations to earn trust in the AI-enabled assets and services provided to the public.

Deloitte's Trustworthy AI™ Framework (Framework) and AI Governance & Risk services help provide strategic and tactical solutions to enable organizations to continue to build and use AI-powered systems while promoting Trustworthy AI (Figure 3).

Deloitte recognizes that organizations and institutions are increasingly adopting AI and automated systems for their potential to revolutionize significant aspects of the American public's daily lives from health care, to banking, to shopping, to leisure downtime, to many more. However, these innovations can be particularly susceptible to a wide range of AI-related risks through all phases of the AI life cycle. For example, AI-based systems may introduce or reinforce a risk of perpetuating inequity and historic bias, and enforceable regulations to protect the American public by ensuring equitable, ethical, and transparent

AI may be not only critical but inevitable. An indication of the future AI regulatory landscape can be seen in recent proposed and enacted state and local laws governing AI in specific use cases, such as AI-based performance evaluation and hiring decisions, loan underwriting models, etc.<sup>6</sup>

Figure 3 | Deloitte’s Trustworthy AI Framework



# Understanding GRMF requirements through Deloitte’s Trustworthy AI™ Framework

Deloitte’s Trustworthy AI Framework (Framework) is in line with CDOI’s draft AI Regulation. The Framework is designed to assist insurance companies in operationalizing automated systems safely and effectively, while protecting individuals and communities and adhering to emerging regulations, such as those provided by CDOI (Figure 4).

Figure 4 | CDOI’s GRMF requirements and how they map to Deloitte’s Trustworthy AI Framework


		Deloitte’s Trustworthy AI™ Framework					
		Fair & Impartial	Robust & Reliable	Privacy	Safe & Secure	Responsible & Accountable	Transparent & Explainable
AI governance and risk management framework	Documented AI governance principals outlining unfair discrimination protections	✓	✓				✓
	Clear roles & responsibilities + oversight					✓	
	Written policies and process for creation, deployment & use of ECDIS and AI models					✓	✓
	Ongoing training and supervision					✓	
	AI models are safe and secure				✓		
	Process and protocol to address consumer inquiries and complaints			✓			✓
	Recovery Plan				✓		
	Audit Plan	✓			✓		✓
Minimum documentation	Inventory of ECDIS and AI models	✓	✓		✓		✓
	Annual Reviews					✓	
	System to track and manage changes		✓				✓
	Testing to detect unfair discrimination	✓	✓				✓
	Identification of potential risks and benefits	✓					
	Vendor selection process					✓	
	Documentation of decisions					✓	
	Regular documentation review					✓	
Reporting Requirements	Report on progress					✓	
	Report on compliance					✓	
	Regular reporting					✓	


The world today is experiencing significant human capacity for insight, decision making, efficiency, and innovation—all dramatically expanded by cognitive systems — during a time in which trust is paramount. The tools that assist in unleashing world changing capabilities should be trusted to act in line with human expectations for ethics and appropriateness. The full potential of AI may hinge on that confidence.


Once finalized and put into effect, the CDOI’s AI Regulation will likely provide specific enforceable requirements for life insurance companies using ECDIS and AI models using ECDIS in Colorado. CDOI has leveraged high-level principles, found in places like the federal regulatory guidelines, and attempted to turn them into reporting requirements for governance, documentation, and reporting. While it is expected to only apply to life insurance companies doing business in Colorado, the draft regulation may set the tone for industry leading practices and other regulators looking to implement similar requirements. Additionally, CDOI has also suggested similar rules may be applied to other insurance lines or other AI or algorithmic uses. We recognize that navigating AI implementation challenges can be complex, and Deloitte Risk & Financial Advisory is committed to helping our clients navigate these challenges agilely while establishing trust with stakeholders and regulators. Deloitte Risk & Financial Advisory, with our suite of AI Governance & Risk assets and services, is dedicated to assisting our clients through the changing regulatory landscape and helping clients create Trust, Equity and Transparency as they serve the American people.

## Where do you start?

As we are waiting for the final regulation<sup>5</sup> to be issued, below are three recommended steps that can help life insurance companies prepare to adhere to the regulatory requirements.

- 

**1** **Conduct a diagnostic assessment** to identify and inventory AI use cases, corresponding purpose (ECDIS and AI models in use) and existing governance & control processes
- 

**2** **Develop an AI governance strategy** with specific outcomes that the company needs to demonstrate compliance, along with a timeline and necessary resources
- 

**3** **Train employees** who work with ECDIS and AI models, to understand new regulatory requirements and identify any policy and / or procedure changes that need to be adopted

Based on the evolving AI regulations landscape across multiple jurisdictions (states), it is important for Risk and Compliance leaders to stay informed about similar regulations that may be implemented in other states and take a holistic approach towards the governance of ECDIS and AI models.

# Contact us for more information



**Oz Karan**  
Risk & Financial Advisory  
Trustworthy AI Leader  
Partner  
Deloitte & Touche LLP  
[okaran@deloitte.com](mailto:okaran@deloitte.com)



**Satish Iyengar**  
Risk & Financial Advisory  
Trustworthy AI – FSI Leader  
Managing Director  
Deloitte & Touche LLP  
[siyengar@deloitte.com](mailto:siyengar@deloitte.com)



**Richard Godfrey**  
Insurance Sector Leader  
Risk & Financial Advisory  
Principal  
Deloitte & Touche LLP  
[rgodfrey@deloitte.com](mailto:rgodfrey@deloitte.com)



**David Sherwood**  
Insurance Regulatory Leader  
Risk & Financial Advisory  
Managing Director  
Deloitte & Touche LLP  
[dsherwood@deloitte.com](mailto:dsherwood@deloitte.com)



## Endnotes

- 1 [White House's Blueprint for an AI Bill of Rights](#)
- 2 [National Institute of Standards and Technology AI Risk Management Framework](#)
- 3 [NAIC 2023 Regulatory Priorities](#)
- 4 [NAIC Principles on Artificial Intelligence](#)
- 5 CDOI draft of [Algorithm and Predictive Model Governance Regulation](#)
- 6 National Conference of State Legislatures [Report on Legislation Related to AI](#)



This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte Risk & Financial Advisory" means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.