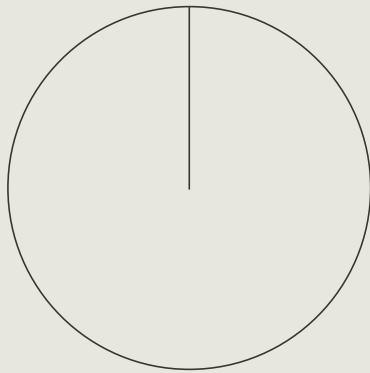


The Colorado AI Act:

A Compliance Handshake Between Developers and Deployers



CO
SB 24-205

Authors

Sheila Leunig
Edward Feldman
Ezra Schwartz
Nadine Dammaschk
Dr. Shea Brown
Dr. Cari Miller
Patrick Sullivan
Abhinav Mittal

Published in August 2025

1 Executive Summary

The Colorado AI Act (Senate Bill 24-205), enacted in 2024 and taking effect on February 1, 2026, establishes the first comprehensive, enforceable state-level framework in the United States for regulating high-risk artificial intelligence (AI) systems. The law imposes clear legal obligations on both developers and deployers of AI systems that significantly impact individuals' access to employment, housing, education, healthcare, and other critical services. Its primary aim is to promote transparency, accountability, and fairness in AI by preventing algorithmic discrimination and create responsible best practices throughout the AI development and deployment lifecycle.

This landmark legislation arrives amid growing global momentum around AI regulation. While federal agencies in the U.S. have issued guidance and voluntary frameworks, Colorado's Act fills a key legislative gap by offering state level enforceable rules tailored to real-world AI use. Internationally, governments and standards bodies are moving in parallel: the EU has adopted its AI Act, and countries such as the UK, Singapore, South Korea, Brazil, Japan and Kenya are advancing their own AI regulatory regimes. Standards like ISO/IEC 42001 and IEEE 3119-2025 provide additional technical scaffolding for organizations to build trustworthy AI systems.

At its core, the Colorado AI Act embraces a modern understanding of governance—not as a bureaucratic constraint, but as a mechanism for responsible value creation and as an enterprise-level process that aligns stakeholder priorities, mitigates risk, and ensures resources are used effectively to achieve intended outcomes. In the context of AI, this means building systems that deliver real benefits while optimizing safety, compliance, and performance. Responsible governance, then, becomes both a foundational responsibility and a business accelerator.

1 Executive Summary

This white paper provides a comprehensive analysis of the Act’s obligations, including the legal duties of developers and deployers, the practical challenges of compliance for both parties, and recommended strategies for managing compliance ambiguities across the AI lifecycle. It also includes a case study and resources to help organizations operationalize their responsibilities under the law.

KEY INSIGHTS



Developer and deployer communication

Compliance under the Act requires close coordination between developers and deployers, including clear documentation, continuous monitoring, and risk mitigation plans.



Internal policies, legal frameworks and contractual agreements

Organizations can resolve interpretive gray areas—such as what constitutes a “substantial modification” or a “reasonably foreseeable” risk—by developing internal policies, legal frameworks, and detailed contractual agreements.



AI governance as value creation

Strong AI governance is a competitive advantage. It protects consumers, reduces legal risk, builds public trust and accelerates responsible innovation.

As the AI regulatory landscape evolves, the Colorado AI Act offers more than just a compliance roadmap. It provides a strategic blueprint for integrating responsible AI practices into the core of business decisions and guardrails that create business value by optimizing operational and financial risks.

2 Overview of the Colorado AI Act (SB 24-205)

The Colorado AI Act mandates transparency and risk management in an effort to mitigate bias discrimination in high-risk AI systems, defined as artificial intelligence systems that make, or are a substantial factor in making, a consequential decision. A “consequential decision” is a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of services or opportunities they have a right to access and receive. Examples of services the Act expressly names as being covered includes legal, insurance, educational, employment and housing opportunities, healthcare, government, and financial services.

The Act requires that developers and deployers of high-risk AI systems exercise reasonable care in avoiding algorithmic discrimination by complying with documentation, disclosure, and monitoring requirements. “Algorithmic discrimination” means any condition in which the use of an AI system results in an unlawful differential treatment or impact that disfavors an individual or groups of individuals based on actual or perceived protected characteristics such as age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classifications protected under the laws of Colorado or federal law.

The Attorney General has exclusive enforcement authority under the Act, and can promulgate rules to implement the law. While comprehensive, the Act also includes exemptions and safe harbors for certain entities.

2 Overview of the Colorado AI Act (SB 24-205)

KEY STAKEHOLDERS



Developer

A person doing business in Colorado that develops or intentionally and substantially modifies an AI system.



Deployer

A person doing business in Colorado that deploys a high-risk AI system.



Consumer

An individual who is a Colorado resident.



Attorney General

The chief legal officer of Colorado, responsible for enforcing the Colorado AI Act.

The phrase “person” is generally interpreted to encompass individuals, corporations, partnerships, and other legal entities. The phrase “doing business in Colorado” implies that the entity operates or provides services within Colorado, regardless of where it is headquartered. And the phrase “intentionally and substantially modifies” refers to a deliberate change made to an AI system that results in any new reasonably foreseeable risk of algorithmic discrimination. For example, such a change could be caused by retraining the system with new data, adding significant features, or changing how it is or can be used.

3 Developer Obligations

Under the Colorado AI Act, developers of high-risk AI systems have a legal obligation to exercise “reasonable care” to avoid algorithmic discrimination by the AI system they develop. Reasonable care is a common legal standard under traditional U.S. tort and regulatory law that implies a context-driven evaluation and requires taking the precautions and actions that a prudent, similarly situated person would take under the same or similar circumstances to prevent harm.

Developers are required to specifically comply with a series of documentation, disclosure, and monitoring requirements aimed at promoting fairness, transparency, and accountability in the use of artificial intelligence. Importantly, developers who meet these obligations are presumed under the law to have met the required standard of acting with reasonable care, creating a strong incentive to comply with the requirements outlined below. By creating thorough documentation, supporting the completion of deployer impact assessments, publishing clear public disclosures, responding to evidence of harm, and committing to continuous maintenance, developers can both comply with the law and demonstrate their commitment to fair, transparent, and accountable AI practices.

3.1 Documentation Requirements

One core obligation the Act places on developers is to prepare and provide detailed documentation for each high-risk AI system they build or substantially modify. This documentation is required to be shared with any deployer—the organization or individual using the high risk AI system—and should be sufficient enough to allow the deployer to understand how the system works and assess its risks.

In addition, developers are required to document how the AI system was tested and evaluated. This includes the key metrics used (whether performance metrics, e.g. accuracy or false positive/negative rates, fairness metrics or other key performance indicators), and any steps taken during development to mitigate bias or discrimination. If human oversight is required for responsible use of the system, the documentation must offer clear guidance on when and how that oversight should be implemented.

3 Developer Obligations

3.1 Documentation Requirements

Developers are expected to disclose any other information necessary for the deployer to understand the system's operation and its potential impact on individuals. Specific exceptions to this obligation include the disclosure of any trade secrets, any information protected by law, and any details that could pose security risks.

3.2 AI Impact Assessment Support

Although the Colorado AI Act places the primary responsibility for conducting formal algorithmic impact assessments on deployers, developers of high-risk AI systems play a vital supporting role.

To enable deployers to fulfill their legal obligations, developers are required to share any documentation, technical specifications, test results, or evaluation materials that are reasonably necessary for a deployer to complete an impact assessment.

This includes:

- a description of how the high-risk AI system was validated
- any known or reasonably foreseeable risks of algorithmic discrimination
- the measures taken to mitigate those risks
- the intended outputs of the high-risk AI system; and
- any demographic performance test results relevant to fairness and system behavior

3 Developer Obligations

3.2 AI Impact Assessment Support

Developers should also share tools or methods that would help deployers evaluate the system within their specific operational context. These requirements can be met using commonly accepted documentation tools such as:



datasheets for datasets

details on data sources, collection methods, and fairness considerations



model cards

model performance limitations, and intended use descriptions



other structured formats

design choices, ethical considerations, training data or model design and evaluation

3.3 Public Disclosure

Under the Colorado AI Act, developers are required to maintain a public-facing disclosure that provides transparency about their high-risk AI systems. The goal of this requirement is to promote transparency and accountability to the broader public, regulators, and potential customers, while creating a record of the developer's approach to responsible AI development. This public statement should be made available on the developer's website or through another accessible platform, and must include two elements: (1) a summary of the types of high-risk AI systems the developer currently offers or has substantially modified, and (2) a description of how the developer manages known or reasonably foreseeable risks of algorithmic discrimination associated with those systems.

This disclosure must be written in plain language and updated within 90 days of any intentional and substantial change to a covered AI system.

3 Developer Obligations

3.4 Discriminatory Incident Reporting

If a developer becomes aware that a high-risk AI system they created or modified has caused or is likely to cause algorithmic discrimination, they are required to report the issue. This includes situations where the developer independently discovers the problem or receives a credible report from a deployer or other third party. In such cases, the developer must notify all known deployers of the relevant system and the Colorado Attorney General within 90 days of discovery. The notice should include a description of the issue, the nature of the potential discrimination, and any actions the developer is taking or has taken to address it. Establishing an internal response protocol for identifying, investigating, and documenting such incidents will help developers meet this obligation in a timely and defensible way.

3.5 Ongoing Updates

Finally, developers are responsible for keeping their technical documentation and public disclosures up to date. Whenever a developer intentionally and substantially modifies a high-risk AI system—such as retraining it with new data, adding significant features, or changing the focus of how it is used—they must update their documentation and public statement within 90 days. This ensures that deployers and the public have access to accurate and relevant information, even as systems evolve.

4 Deployer Obligations

Under the Colorado AI Act, deployers of high-risk AI systems, like developers, are also required to exercise reasonable care to protect consumers from any known or reasonably foreseeable algorithmic discrimination risks. This duty includes implementing and maintaining a policy and program for responsible AI management, conducting AI impact assessments, publishing notices and disclosures, and ensuring ongoing monitoring of the high-risk AI systems they deploy. Deployers who meet these obligations are presumed under the law to have met the required standard of acting with reasonable care, again creating a strong incentive to implement the practices described below.

4.1 Risk Management Policy and Program

The Colorado AI Act requires deployers of high-risk AI systems to establish and maintain both a risk management policy and a risk management program to identify, mitigate, and monitor risks of algorithmic discrimination across the high-risk AI system's lifecycle.

The risk management policy must:

- articulate the principles guiding responsible AI governance within the organization
- define how the deployer will identify, document, and address known or reasonably foreseeable risks of algorithmic discrimination
- outline the processes used to manage those risks
- identify the personnel responsible for implementing and overseeing risk mitigation efforts

This policy serves as the foundational statement of how the deployer approaches AI risk governance.

4 Deployer Obligations

4.1 Risk Management Policy and Program

The risk management program must:

- be actively planned, implemented, and regularly reviewed and updated over the lifecycle of the high-risk AI system
- reflect guidance from well-established AI governance frameworks, such as the **NIST AI Risk Management Framework**, **ISO/IEC 42001**, or other nationally or internationally recognized frameworks designated by the Colorado Attorney General
- be tailored to the deployer's specific context, considering the organization's size and operational complexity, the nature and scope of the high-risk AI system, including its intended uses and specific deployment contexts and the sensitivity and volume of data used

This program operationalizes the risk policy by embedding oversight and accountability into day-to-day AI use. A deployer that establishes and follows a risk management policy and program that is compliant with the Colorado AI Act requirements is presumed to have exercised “reasonable care” in preventing algorithmic discrimination. This can serve as a defense in enforcement actions brought by the Colorado Attorney General, provided the deployer can demonstrate adherence to the governance requirements.

4.2 AI Impact Assessment

Deployers of high-risk AI systems are required under the Colorado AI Act to conduct thorough algorithmic impact assessments to evaluate and manage the risk of algorithmic discrimination.

Deployers must:

- complete an initial impact assessment before deploying a high-risk AI system
- conduct an annual review of the assessment's findings; and
- update the assessment within 90 days of making any intentional and substantial modification to the AI system

4 Deployer Obligations

4.2 AI Impact Assessment

Each impact assessment must document:

- the purpose of the high-risk AI system and its intended use cases
- any known or foreseeable risks of algorithmic discrimination, along with mitigation strategies
- the categories and sources of data used in the system
- the key metrics used (performance metrics, fairness metrics or other key performance indicators) and known limitations
- any transparency measures implemented; and
- the post-deployment monitoring and safeguards in place

If the system is substantially modified at a later date, the assessment must be updated to include an explanation of how the AI system's actual use continues to align with its originally intended purpose.

To enable accurate and complete assessments, the Colorado AI Act requires developers to provide deployers with all reasonably necessary documentation, including:

- technical specifications
- test results
- evaluation materials; and
- any other supporting artifacts (e.g., model cards or dataset summaries)

4 Deployer Obligations

4.2 AI Impact Assessment

Given that a deployer's ability to comply with the impact assessment requirement relies on information disclosed by developers, it is of the utmost importance for deployers to be organized and proactive, for example, double checking with their vendor developers that all necessary information has been disclosed at the time a contract for use of the underlying AI system is signed.

Deployers may use a single impact assessment to cover multiple comparable high-risk AI systems if they can document why the systems are substantially similar. They may also rely on impact assessments completed under other legal frameworks provided they are equivalent in scope and rigor to the requirements for impact assessments under the Act.

4.3 Public Disclosure

Deployers of high-risk AI systems operating within Colorado must provide clear notifications to consumers before these systems make or substantially influence consequential decisions. When deploying such systems, deployers must inform consumers about the system's purpose, describe the system in plain language, explain opt-out rights, and provide contact information. Additionally, any AI system that interacts with consumers must disclose its artificial nature unless obvious to a reasonable person. For systems that may produce adverse decisions for consumers, deployers must disclose the reasoning behind the decision, including how the AI contributed, what data was used, data sources, and offer opportunities to correct personal data and appeal decisions with human review when feasible.

Deployers must maintain a publicly accessible inventory on their website detailing their high-risk AI systems. This disclosure must also include what information the AI systems collect and how the organization manages discrimination risks. This inventory requires periodic updates. If algorithmic discrimination is discovered within any of the AI systems, deployers must notify the Colorado Attorney General and affected consumers within 90 days.

4 Deployer Obligations

4.3 Public Disclosure

Regardless of the type of notification or disclosure, all notices must be provided in plain language, in all languages the deployer typically uses for consumer communications, and in accessible formats for people with disabilities.

4.4 Deployment Monitoring and AI Audits

Organizations must implement comprehensive post-deployment risk management processes that include ongoing monitoring, user safeguards, oversight mechanisms, usage tracking, and learning processes. These requirements establish a framework for continuous evaluation and improvement of high-risk AI systems to prevent discriminatory outcomes and manage risks throughout the system's lifecycle. For added assurance, either the deployer or a third party contracted by the deployer must conduct a review annually of each AI system to verify that the system is not causing algorithmic discrimination.

5 Exemptions and Special Circumstances

While the Colorado AI Act establishes one of the most comprehensive regulatory frameworks in the United States for high-risk AI systems, it also recognizes the need for flexibility in its application. To avoid imposing disproportionate burdens and to ensure consistency with existing federal and sectoral oversight regimes, the Act includes targeted exemptions and carve-outs based on organizational size, domain-specific regulation, and the nature of certain AI applications.

This section outlines the specific categories of exemptions—ranging from small business accommodations to federally regulated sectors—and clarifies the legal protections that remain intact for developers and deployers. These exemptions are designed to support innovation, reduce compliance friction for low-risk or highly regulated entities, and ensure the law operates in harmony with broader legal and operational frameworks.

5.1 Organizational Size Exemption

Deployers with fewer than 50 full-time employees that do not use their own data to train high-risk AI systems qualify for a limited compliance exemption under the Colorado AI Act. This exemption applies when using high-risk AI systems that have been trained only on data from external sources, for example, pre-trained models that used data collected by a developer.

Additionally, this exemption extends to deployers when they use the high-risk AI system for their intended and disclosed purpose, as defined by the developer. Qualifying deployers can provide the developer's impact assessment to the Attorney General instead of creating their own, and are exempt from the Colorado AI Act obligations to update risk management policies and programs, conduct impact assessments, and disclose their inventory of high-risk AI systems.

5.2 Special Circumstances by Domain

The Colorado AI Act includes targeted exemptions for deployers and developers who are operating in certain federally regulated sectors or are already subject to rigorous oversight. These exemptions aim to avoid duplicative regulation where equivalent or stronger protections are already in place.

5 Exemptions and Special Circumstances

5.2 Special Circumstances by Domain

+ **Federal Agency Compliance**

AI systems approved or developed by the Food and Drug Administration (FDA), Federal Aviation Administration (FAA), or Federal Housing Finance Agency are exempt if those agencies impose risk mitigation standards equal to or stricter than the Colorado AI Act.

+ **Federal Contracts**

High-risk AI systems developed under contract with the Department of Commerce, Department of Defense, or NASA are exempt unless used for employment or housing decisions.

+ **Research Systems**

High-risk AI systems used solely for research and development to support regulatory submissions to agencies like the FDA, FAA, or Federal Communications Commission (FCC) are exempt.

+ **Healthcare**

Entities covered by the Health Insurance Portability and Accountability Act (HIPAA) are exempt when AI-generated recommendations are required to be reviewed and acted upon by a healthcare provider and are not deemed high-risk.

+ **Insurance**

Insurers and their developers are exempt if they comply with Colorado's previously existing insurance regulations (specifically, C.R.S. § 10-3-1104.9) regarding anti-discrimination, which include obligations to assess AI systems for bias and report mitigation efforts to the state Division of Insurance.

+ **Banking**

Banks, credit unions, and affiliates are exempt if they are subject to regulatory audits that address algorithmic discrimination risks and meet or exceed the Act's requirements.

5 Exemptions and Special Circumstances

5.3 Untouched Legal Protections

It is interesting that the Colorado AI Act also outlines important clarifications about what it does not seek to restrict developers and deployers from doing.

Permissible activities include:

- trade secret protection, provided consumers are notified when information is withheld
- compliance with with governmental inquiries, investigations, or regulatory obligations
- cooperation with law enforcement in connection with lawful investigations.
- protection of essential safety interests, such as responding to emergencies or threats
- maintenance of system security, including cybersecurity and operational integrity
- following applicable research ethics and privacy laws
- conducting real-world testing of AI systems prior to full deployment
- implementing product recalls where necessary to address risk or harm
- fixing technical errors or malfunctions in AI systems
- exercising freedom of speech and press, consistent with constitutional protections

These provisions ensure that while the Colorado AI Act imposes certain AI governance requirements, it also works to preserve necessary operational freedoms for organizations developing and deploying AI systems.

6 Challenges to Compliance

While the Colorado AI Act establishes a forward-looking framework for regulating high-risk AI systems, it also introduces considerable areas of legal and operational uncertainty for both developers and deployers. Many of the terms and obligations within the Act are open to interpretation, raising questions about how to implement its provisions consistently and effectively. This section outlines some of the key compliance challenges emerging from the Act and offers practical approaches for addressing them.

6.1 Ambiguity Around the “Foreseeability” of Risk

One of the central duties in the Colorado AI Act is the obligation of developers and deployers to exercise “reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination.” However, the Act does not provide a definition or clear criteria for what constitutes a “foreseeable” risk. This ambiguity creates uncertainty about how far an organization’s duty of care extends, particularly when dealing with novel or complex AI systems.

To address this challenge, organizations can adopt internal governance frameworks that consider how the AI system might cause different risks of algorithmic discrimination for different groups of affected stakeholders, and evaluate and prioritize the identified risk based on the likelihood and severity of potential harm. Drawing from legal precedent or pending litigation in product liability and privacy law, companies can implement structured risk assessments that identify known use cases where algorithmic discrimination has historically occurred, such as in hiring, lending, or medical triage systems.

For example, a deployer using an AI-powered resume screening tool should proactively assess whether the system penalizes candidates with employment gaps, a practice that may disproportionately affect women or older applicants. By incorporating cross-functional input from legal, product, and ethics teams, organizations can better identify risks that a reasonable entity in their position should have foreseen.

6 Challenges to Compliance

6.2 Lack of Clarity Around “Substantial Modifications”

The Act requires deployers to update their impact assessments whenever a high-risk AI system undergoes a “substantial modification.” Yet the term “substantial modification” itself is not specifically defined within the legislation, leaving room for interpretive inconsistencies. Organizations will struggle to determine when changes to system architecture, inputs, or functionality rise to the level of being “substantial” and thus trigger new compliance obligations.

To manage this ambiguity, organizations should create internal policies that define and establish materiality thresholds for AI system changes. For example, a material change might include retraining the model with a new dataset, introducing new decision-making logic, or expanding the AI system’s use into a different risk domain. Conversely, minor updates that do not significantly alter output behavior may be excluded from these triggers. For example, a financial institution modifying an AI tool to incorporate new demographic data fields—without changing its core decision logic—might still treat the change as substantial, given the likelihood of affecting fairness outcomes.

6.3 Developer Obligations to Share Information

Several sections of the Colorado AI Act require developers to provide deployers with information “necessary” for deployers to meet their legal obligations. However, the statute does not specify what qualifies as “necessary” other than to say “...any other documentation reasonably necessary to assist the deployer in understanding the AI system’s outputs and monitoring its performance for risks of algorithmic discrimination.” The lack of specificity in this requirement of the Act creates tension between a developer’s desire to maximize efficiencies and protect proprietary information and the deployer’s need for transparency to ensure legal compliance.

6 Challenges to Compliance

6.3 Developer Obligations to Share Information

This can lead to practical roadblocks, particularly when deployers are held accountable for systems they did not build and do not fully control. To mitigate this, developers and deployers should align on standardized disclosure protocols at the outset of their business relationships, for example, they can agree on an obligation to deliver a previously agreed upon list of documents upon execution of the contract governing their relationship. Regardless, developers must provide documentation that includes the high-risk AI system's intended use cases, known limitations, relevant training data categories, key metrics used, and mitigation strategies, and a signed attestation that the system has been tested for algorithmic discrimination in line with the requirements of the Colorado AI Act.

In turn, deployers should formalize information-sharing expectations in their commercial contracts with developers to include obligations to share detailed documentation, validation results, and updates following any substantial modifications to the AI system. Contracts should also address the need for support for impact assessments, prompt notification of any discriminatory outcomes, and cooperation in remediation and regulatory disclosures. Additional terms may include indemnification for compliance failures, audit rights, public disclosure coordination, and clear procedures for protecting trade secrets while meeting legal obligations. These clauses help ensure that deployers can meet their risk management, transparency, and accountability duties under the Act, including provisions for updates following substantial modifications.

The Colorado AI Act ties developers and deployers together through what is, in effect, a compliance handshake. Developers are expected to provide deployers with all “reasonably necessary” information—model-level documentation, data summaries, evaluation results and known limitations—whenever they offer or substantially modify a high-risk AI system. Deployers, by contrast, cannot deploy that same AI system until they have built and instituted a risk management policy and program, and completed an impact assessment that relies entirely on the developer's materials. The statutory logic is straightforward: one party supplies facts; the other translates those facts into accountable operations.

6 Challenges to Compliance

6.3 Developer Obligations to Share Information

Where the relationship gets complicated is in the space between these two statutory duties. Developers are allowed to redact trade secrets or security-sensitive details without breaching the Act, while deployers remain fully liable for an incomplete or inaccurate impact assessment. If new risks are introduced into a high risk AI system when the deployer fine-tunes the model or lets it continue learning after deployment, new assessments must be run, and as a result the original documentation may become outdated and no longer accurately describe the system that is actually in production.

Under the Act, smaller deployers—those with fewer than fifty employees—are exempt from the policy, assessment, and web-posting requirements so long as they do not train the AI system on their own data. While this eases their compliance burden, it also unintentionally creates gaps for developers whose own obligations may depend on deployer input. For example, without an impact assessment from deployers, developers lose visibility into how their AI systems are performing in real-world conditions, weakening their ability to update their own documentation. Exempt deployers also have no duty to conduct ongoing monitoring, depriving developers of valuable performance and bias data needed for their disclosures. Finally, both parties have ninety days to alert the Attorney General if they discover discriminatory outcomes in a high-risk AI system they are using, but only the developer is expressly obliged to notify its deployer counterpart, creating awkward questions about who speaks first when something goes wrong

Businesses can again smooth these fault-lines by mutually agreeing on information sharing obligations in their commercial contracts. Developers should commit to share detailed evaluation artifacts, refresh model cards or dataset sheets whenever significant updates occur, and provide rapid answers to deployer follow-up questions.

Deployers, in turn, should formalize how and when they will request deeper technical detail and reserve the right to commission an independent audit if critical gaps persist. Joint implementation workshops, followed by annual or post-update meetings, help keep the developer’s “intended uses” and the deployer’s real-world context aligned, while API-level telemetry or shared dashboards can flag performance drift before it escalates into liability. Treating the Act’s documentation requirements as an ongoing, contractual deliverable rather than a one-time hand-off turns the statutory compliance handshake into an operational partnership that lowers risk for both sides.

6 Challenges to Compliance

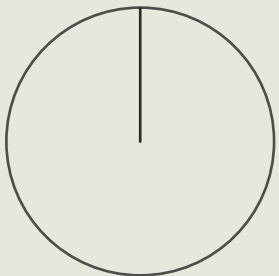
6.4 Flexibility Without Standards in Bias Testing

The Colorado AI Act requires deployers to measure and mitigate algorithmic discrimination, but does not prescribe specific testing methods, performance thresholds, or benchmark datasets to determine when algorithmic discrimination has occurred. While this flexibility allows for domain-specific adaptation, it also introduces ambiguity in compliance that will result in inconsistency and the risk of underenforcement. For example, some deployers may adopt superficial or biased evaluation frameworks while still claiming compliance to protect against discrimination, thereby undermining the intent of the law.

These metrics should be tailored to the high-risk AI system's use case and accompanied by representative data that reflects the diversity of the affected population. For example, a healthcare provider deploying an AI-based diagnostic support system should evaluate its performance across demographic subgroups to ensure that referral rates or treatment recommendations do not vary inappropriately by race, gender, or age or sexual orientation. All testing procedures and outcomes should be documented and required as part of the impact assessment process, with clear justification for the metrics and methods chosen.

The Colorado AI Act sets an important precedent for AI accountability, but its effectiveness hinges on how well developers and deployers navigate its ambiguities together. Undefined terms like “foreseeable risk” and “substantial modification,” inequitable responsibilities, and lack of mandated bias testing standards creates real compliance challenges. To meet the Act's obligations, developers and deployers must adopt clear internal policies, align contracts and documentation, and commit to ongoing proactive, cross-functional oversight. Success will depend not just on legal compliance, but on building systems that are genuinely fair, transparent, and trustworthy.

7 Conclusion

compliance	key challenges
	<ul style="list-style-type: none">ambiguous compliance requirementsundefined termsgaps in documentationadoption of clear internal policiescontract alignment

The Colorado AI Act is a landmark piece of legislation and the first in the United States to establish a comprehensive, enforceable framework for the regulation of high-risk AI systems at the state level. By setting clear legal obligations for both developers and deployers, the Act provides a detailed model for how principles like accountability, transparency, and fairness can be translated into concrete governance practices. It establishes a strong precedent for other jurisdictions seeking to build regulatory systems that protect the public while enabling responsible AI innovation.

Three key takeaways emerge from the analysis in this white paper. First, from the start, developers and deployers must treat compliance as a shared responsibility, proactively coordinating on documentation, disclosures, and risk management to meet their respective legal duties. Second, developers and deployers should address the Act’s interpretive ambiguities, for example as to what constitutes a “substantial modification” or “reasonably foreseeable” risk, through internal policies, legal guidance, and carefully drafted commercial agreements. Third, leveraging existing recognized frameworks for the governance of AI systems like ISO 42001, 42005, and the NIST AI Risk Management Framework can help companies standardize their compliance approach under the Act, resolve existing ambiguities in the law, and demonstrate the standard of reasonable care.

Ultimately, sound AI governance is both a compliance obligation and a business imperative. It safeguards consumers, reduces legal and reputational risk, fosters public trust, and enables organizations to deploy AI systems confidently and responsibly. The Colorado AI Act offers a roadmap for building AI ecosystems that are not only legally defensible, but also safe, inclusive, and innovation-ready.

Resources

- + **Developer Obligations Checklist**
- + **Deployer Obligations Checklist**
- + **AI Impact Assessment Template**
- + **MLOps Compliance Deliverables**
- + **Case Study**

The Colorado AI Act developer obligations

This checklist outlines the steps developers can take to comply with the Colorado AI Act. It assumes that no exemptions under the Colorado AI Act apply, and it is intended for legal, compliance, and technical leads responsible for high-risk AI systems.

Who is a Developer?

Anyone doing business in Colorado who builds or substantially modifies a high-risk AI system. Doing business in Colorado implicates entities operating, providing services, or selling product in Colorado regardless of their headquarters.

What is a High-Risk AI System?

Any AI tool that plays a key role in consequential decisions about people's access to jobs, housing, education, loans, insurance, legal services, healthcare, or government benefits.

Primary Obligations

Documentation and Disclosures to Deployers

Public Notices and Disclosures

Support for Deployer Impact Assessments

Monitor and Report Algorithmic Discrimination

Maintain Up-To-Date Documentation

Documentation and Disclosure to Colorado Attorney General

Documentation to submit to deployers

A general statement of the AI system's intended purpose, intended benefits, reasonably foreseeable uses, and known harmful or inappropriate uses

A description of the types of data used to train the AI system, and any known or foreseeable limitations

A description of how the AI system was tested and evaluated, including metrics used, known limitations, and any steps taken to test for and mitigate algorithmic discrimination

A description of data governance and risk mitigation practices applied during development

Instructions for responsible deployment, including any recommendations for human oversight, ongoing monitoring, and user safeguards

Any other technical documentation necessary for the Deployer to understand the AI system's outputs and limitations

The Colorado AI Act

deployer obligations

This checklist outlines the steps deployers can take to comply with the Colorado AI Act. It assumes that no exemptions under the Colorado AI Act apply, and it is intended for legal, compliance, and technical leads responsible for high-risk AI systems.

Who is a Deployer?

A person doing business in Colorado that deploys a high-risk AI system. Doing business in Colorado implicates entities operating, providing services, or selling product in Colorado regardless of their headquarters.

What is a High-Risk AI System?

Any AI tool that plays a key role in consequential decisions about people's access to jobs, housing, education, loans, insurance, legal services, healthcare, or government benefits.

Primary Obligations

- Establish and maintain an AI Risk Management Policy and Program

- Conduct Algorithmic Impact Assessments

- Provide Pre-Use Consumer Notices and Disclosures

- Maintain Public Inventory of High-Risk AI Systems

- Monitor AI System Performance Post-Deployment

- Investigate and Report Algorithmic Discrimination

- Maintain Updated Disclosures and Assessment Materials

Detailed compliance requirements

Risk Management Policy and Program

- Create a documented risk management policy that defines governance principles, roles, and responsibilities

- Implement a risk management program aligned with national or international frameworks (e.g., NIST AI RMF, ISO/IEC 42001)

- Regularly review and update both the policy and the program

Algorithmic Impact Assessments

- Complete an initial impact assessment before deploying a high-risk AI system

- Include the AI system's purpose, data sources, risks of algorithmic discrimination, mitigation steps, limitations, and performance metrics

- Update the assessment within 90 days of any substantial modification

- Conduct a review at least annually

- Ensure assessments are supported by technical documentation from the Developer

What is an AI Impact Assessment?

The AI impact assessment required of developers under the Colorado AI Act is a methodical review of impacts that may not surface through technical testing or standard business planning. It creates a record of what was known at the time decisions were made about the development or deployment of an AI system, which helps establish accountability over time. Ultimately, it will help your organization identify how its AI systems may affect people and it is considered an established AI governance best practice. For example, the ISO/IEC 42001 AI Management System standard also requires that organizations conduct AI impact assessments, which are outlined in further detail in ISO/IEC 42005.

Once the assessment is completed, the output should not remain static as findings can directly support the improvement of your organization's broader risk treatment processes. If the assessment identifies potential harm to specific stakeholder groups, that insight should inform control design, policy changes, or access restrictions. If the system introduces new risks that affect regulatory posture or contractual commitments, those risks should be documented and addressed through existing governance mechanisms.

The results of an assessment should also be included in your leadership team's regular review of the organization's risk profile as a whole. This ensures that leadership is informed about the real-world impacts of deployed systems and can adjust strategy or resource allocation if needed. Where gaps are identified between documented expectations and real-world deployment, those gaps should be tracked as nonconformities or improvement actions. This helps the organization maintain a credible and responsive approach to AI governance, especially in environments where systems evolve quickly or operate across business units.

By using the output of the impact assessment as an input to continuous oversight, your organization moves beyond point-in-time analysis, ad hoc and reactive, into sustained, proactive risk management.

section	description	response
AI System Identification	What is the name or common reference used for this AI system?	
Lifecycle Stage	At what stage is this AI system (e.g., design, testing, implementation)?	
System Description Plain English)	Describe what the AI system does in plain terms	
System Purpose	What business or user goal does this system help achieve?	
Intended Use Cases	Where and how is the AI system expected to be used? Who is expected to use it?	
Known Misuse Scenarios	Describe foreseeable unintended uses or misuse scenarios	
Relevant Data Sources	List datasets used (e.g., customer data, transaction logs, third-party sets)	
Data Privacy and Quality Concerns	Are there known quality issues, privacy risks, or data limitations?	
Model or Algorithm Used (if known)	Name the model/algorithm (if known) and any key performance expectations	
Intended Deployment Environment	Where will this AI system be deployed? What systems does it rely on?	
Impacted Stakeholders (Internal & External)	List anyone who may be affected, including employees, customers, or the public	
Benefits to Stakeholders	What are the expected benefits for each group?	
Potential Harms to Stakeholders	What are the realistic risks or harms that could arise?	
Mitigations or Safeguards Planned	What actions are planned to reduce or prevent the potential harms?	
Assessment Completion Date	When was this assessment completed or last updated?	
Reviewer(s) and Approver(s)	List names and roles of those who completed, reviewed, and approved it.	

The Colorado AI Act

MLOps Compliance Deliverables

A comprehensive 180-day roadmap for AI system developers and deployers working towards compliance with the Colorado AI Act. Specifically written for technology professionals, DevOps teams and DataOps engineers.

MLOps Lifecycle	Key Deliverables	CO AI Act Ref #
30 DAYS		
+ Model Governance & Planning	AI System Inventory & High-Risk Classification Matrix	6-1-1702(1)
+ Model Governance & Planning	AI Governance Team Charter & RACI Matrix	6-1-1702(1)
+ Model Governance & Planning	Legal Compliance Assessment & Gap Analysis	6-1-1702(1)
+ Data Engineering & Model Development	Technology Architecture Documentation & Tool Selection	6-1-1702(2)(b)
+ Data Engineering & Feature Engineering	Data Lineage Documentation & Training Dataset Summaries	6-1-1702(2)(b)(I)
60 DAYS		
+ Model Governance & Risk Management	NIST AI RMF or ISO 42001 Framework Implementation	6-1-1702(1)
+ Model Development & Documentation	Standardized Model Cards & Documentation Templates	6-1-1702(2)(c)
+ Model Registry & Version Control	Model Registry Setup & Version Control Processes	6-1-1702(4)(a)
+ Model Validation & Testing	Bias Detection Pipelines & Testing Protocols	6-1-1702(2)(c)(I)
+ Data Engineering & Governance	Data Governance Policies & Access Controls	6-1-1702(2)(c)(II)
90 DAYS		
+ CI/CD & Model Deployment	Automated Documentation Pipeline with CI/CD Integration	6-1-1702(2)(d)
+ Model Monitoring & Observability	Bias Monitoring Dashboards & Alert Mechanisms	6-1-1702(2)(c)(V)
+ Model Governance & Transparency	Public Transparency Website & Statement Updates	6-1-1702(4)
+ Model Monitoring & Incident Management	Incident Response Playbook & Escalation Procedures	6-1-1702(5)
+ Model Serving & API Management	Deployer Communication APIs & Integration Documentation	6-1-1702(3)(a)
120 DAYS		
+ Model Serving & Integration	Impact Assessment Support APIs & Integration Tools	6-1-1702(3)(a)
+ Model Monitoring & Analytics	Advanced Analytics Dashboards & Performance Reports	6-1-1702(7)
+ Model Governance & Compliance	Automated Compliance Monitoring System & Alerts	6-1-1702(1)
+ Model Validation & Testing	Pre-deployment Readiness Testing & Certification	6-1-1702(1)
180 DAYS		
+ Model Deployment & Production	Production-Ready System & Final Integration Testing	6-1-1702 (all)
+ Model Operations & Maintenance	Staff Training Materials & Knowledge Transfer Documentation	6-1-1702 (all)
+ Model Governance & Documentation	Go-Live Checklist & Final Documentation Package	6-1-1702(4)(b)
+ Model Monitoring & Operations	Ongoing Monitoring Setup & Maintenance Procedures	6-1-1702(5)

The Policy Update

The Policy Update is a community of continuous learners working at the intersection of AI, law, science, and society. United by a shared commitment to Responsible AI, we bring together diverse expertise to explore complex challenges, conduct meaningful research, and engage in thoughtful dialogue. Our goal is to inform policy, advance understanding, and help shape AI's development and deployment in ways that benefit society.

Authors

Sheila Leunig

Sheila Leunig is an attorney with over 20 years experience helping emerging tech startups scale, navigate risk, and lead responsibly at the intersection of law and innovation. She specializes in building right-sized legal infrastructure, aligning legal strategy with business goals, and operationalizing AI governance. A former General Counsel to both public and private companies, she now provides fractional GC services, advises the UC Berkeley Law AI Institute, and co-hosts Not Another AI Podcast with Women Defining AI.

Edward Feldman

Edward Feldman is a creative strategist, certified AI auditor and responsible AI practitioner with over 20 years experience in multi-platform storytelling. His responsible AI advocacy work extends to contributions with ForHumanity and the International Association of Algorithmic Auditors (IAAA).

Ezra Schwartz

Ezra Schwartz is a product strategist, UX designer, and certified AI auditor with three decades of experience in human-centered innovation. He specializes in age-inclusive research and service design, helping AgeTech companies and care providers build AI-driven solutions that enhance dignity and connection. An advocate for responsible AI, he guides organizations in implementing ethical UX practices and governance frameworks. Ezra has authored three books on UX, holds a design patent, and champions people-first design that balances technology with compassion.

Authors

Nadine Dammaschk

Nadine Dammaschk is an advisor on AI governance and data privacy in international cooperation. With over 5 years of experience in responsible AI, she specializes in assessing the impact of AI systems from a socio-technical perspective and operationalizing AI risk management. A certified Data Ethics Professional and AI Auditor, Nadine contributes to the development of AI auditing standards through the International Association of Algorithmic Auditors (IAAA).

Dr. Shea Brown

Dr. Shea Brown is founder and CEO of BABL AI and an internationally recognized expert in AI auditing, bias in machine learning, and AI governance. He advises on AI regulations in the U.S. and EU, and is a Fellow and Board member at ForHumanity, a nonprofit setting standards for algorithm auditing and governance. A founding member of the International Association of Algorithmic Auditors, he is helping to advance the algorithmic auditing profession. Former professor of Astrophysics at the University of Iowa, his research focused on machine learning in astrophysical applications.

Dr. Cari Miller

Head of AI Governance and Policy at The Center for Inclusive Change and Executive Director of the AI Procurement Lab. Cari is a globally recognized AI risk expert, AI procurement coach, and consultant. She advises organizations on AI risk management, governance considerations, workforce impact planning, and AI upskilling. She is a certified ISO/IEC 42001 Lead AI Auditor, a certified organizational change manager, and an adjunct professor of AI leadership at Wilmington University in Delaware.

Patrick Sullivan

Patrick Sullivan is the VP of Strategy & Innovation at A-LIGN, specializing in AI Governance, IT security, and compliance. With over 25 years of experience in the industry, Patrick focuses on providing strategic guidance and support to our customers and partners, helping them navigate the complex and evolving landscape of AI governance, cybersecurity, and compliance. His expertise is instrumental in aiding organizations to achieve their strategic security and compliance goals effectively.

Authors

Abhinav Mittal

Abhinav Mittal is an AI Strategy & Governance Advisor with over 20 years of experience in enterprise technology. He advises CXOs and public sector leaders on Gen AI strategy, value realization, and Responsible AI, translating global governance principles into board-level strategies, operating models, and risk controls. An award-winning published author and certified ISO 42001 Lead Implementer, he has contributed to global AI standards through IEEE, ForHumanity, and All Tech Is Human. His work bridges GenAI execution with governance, ensuring AI solutions are scalable, auditable, and outcome-driven.