AI Compliance Landscape

ISO/IEC 42001, NIST AI RMF, EU AI Act, Colorado AI Act. ✅ yes, 🟡 partial, ❌ no.

Optimized for LinkedIn document carousel, 1080 × 1350 per page.

Governance

Scope & status | Roles | Coverage

Question	ISO 42001	NIST AI RMF	EU AI Act	Colorado AI Act
Is it legally mandatory?	❌ **Voluntary, certifiable**	❌ **Voluntary guidance**	✅ **Binding EU law**	✅ **State law**
When is it effective?	**Dec 2023** publication, certification 2024+	**Jan 26, 2023**	**Phased**, bans Feb 2025, GPAI Aug 2025, most high risk Aug 2026, some 2027	**June 30, 2026**
Do we need an organization wide AI program?	✅ **AI management system**	✅ **Governance framework**	✅ **QMS & risk mgmt for high risk**	✅ **Risk mgmt program**
Are accountability roles defined?	✅ **Roles & RACI**	✅ **Governance team**	✅ **Provider, Deployer, Distributor, Importer**	✅ **Developer, Deployer**
Does it cover the public sector?	✅	✅	✅ **Public bodies as deployers**	🟡 **Mostly private, exemptions apply**
Does it cover the private sector?	✅	✅	✅	✅

Risk & Controls

Risk program | Human oversight | Assurance

Question	ISO 42001	NIST AI RMF	EU AI Act	Colorado AI Act
Is a continuous risk management program required?	✅ Comprehensive	✅ Mapping & treatment	✅ Mandatory for high risk	✅ Ongoing risk evaluation
Is there an inventory of systems and uses?	✅ Use case register	✅ Inventory encouraged	✅ High risk inventory & PMS	✅ Website statements, impact assessments
Is human oversight mandatory?	✅ Responsibilities defined	✅ Human in the loop	✅ Intervention mechanisms	✅ Review adverse outcomes when feasible
Are secure by design controls required?	✅	✅	✅	🟡 Implied
Are third party assessments required?	🟡 Via ISO certifiers	❌	✅ Notified Body for many high risk	❌

Data, Testing & Quality

Data lifecycle | Testing | Monitoring

Question	ISO 42001	NIST AI RMF	EU AI Act	Colorado AI Act
Does it require data governance?	✅ Lifecycle controls	✅ Integrity & quality	✅ Quality & representativeness	🟡 Not explicit
Is pre deployment testing required?	✅	✅	✅ Conformity for high risk	🟡 Bias & discrimination tests
Is post deployment monitoring required?	✅ Internal audits	✅ Continuous monitoring	✅ Post market monitoring	✅ Annual reviews
Are evaluation metrics tracked?	✅	✅	✅ Test logs & records	🟡 When risks present

Documentation & Transparency

Technical file | Disclosures | Traceability

Question	ISO 42001	NIST AI RMF	EU AI Act	Colorado AI Act
Is technical documentation required?	✅ System documentation	✅ System context & decisions	✅ Technical file & logs	✅ Document risk controls
Are user disclosures required?	🟡 Policy driven	🟡 Explainability focus	✅ User transparency duties	✅ Notices before consequential decisions
Is public registration required?	❌	❌	✅ EU database for high risk	❌
Are traceability & audit trails required?	✅	✅	✅	🟡 Basic records

Reporting & Enforcement

Incidents | Certification | Penalties

Question	ISO 42001	NIST AI RMF	EU AI Act	Colorado AI Act
Is serious incident reporting mandatory?	🟡 Internal policy	🟡 Voluntary feedback	✅ Max 15 days from awareness, shorter in some cases	✅ Notify AG within 90 days of discovered discrimination
Is there a conformity or certification mark?	✅ ISO certificate	❌	✅ CE marking for high risk	❌
What are the maximum penalties?	N/A	N/A	Up to €35M or 7% global turnover	Up to $20,000 per violation
Can authorities audit or do market surveillance?	❌	❌	✅ Competent authorities, Notified Bodies	✅ AG enforcement