AI Governance Compliance Handbook

Global Regulatory Framework for US, EU & APAC Markets

Executive Summary - Immediate Action Required

Critical Timeline: US federal agencies must implement AI safeguards by December 1, 2024, or discontinue use. EU AI Act general application begins August 2, 2026. Colorado AI Act compliance required by June 30, 2026.

30-Day Action Items

- ☐ Form AI Governance Board and appoint Chief AI Officer (CAIO)
- ☐ Complete comprehensive AI system inventory with risk classifications
- ☐ Freeze high-risk deployments lacking impact assessments
- ☐ Establish incident reporting procedures with 15/2/10-day EU timers
- ☐ Implement NIST AI Risk Management Framework baseline controls

90-Day Priorities

- ☐ Deploy bias audit processes for hiring AI (NYC Local Law 144)
- ☐ Establish content provenance pipeline for Generative AI
- ☐ Map high-risk use cases to EU AI Act categories
- ☐ Implement China Generative AI Measures for APAC operations
- ☐ Set up vendor recertification program for third-party models

Table of Contents

5. Vendor Evaluation Frameworks
6. Audit Preparation Checklists
7. Risk Mitigation Strategies
8. Policy Template Libraries
9. Compliance Roadmaps
10. Enforcement Mechanisms
11. Sector-Specific Requirements

1. Regulatory Landscape Mapping

European Union

AI Act Status: In force since August 1, 2024. Phased implementation with prohibitions beginning 2025, general application August 2, 2026, and Article 6(1) risk-scoping from 2027.

Provision	Effective Date	Key Requirements
Prohibitions & AI Literacy	2025	Banned AI practices, mandatory literacy training
GPAI Model Obligations	August 2, 2025	Systemic risk evaluation, documentation, incident reporting
General Application	August 2, 2026	High-risk AI conformity assessments, post-market monitoring

Penalties: Up to €35M or 7% of global turnover for prohibited practices; €15M or 3% for operator obligations; €7.5M or 1% for misleading information.

United States

Federal Requirements: OMB M-24-10 mandates Chief AI Officers, AI inventories, and minimum safeguards by December 1, 2024, with stop-use enforcement for non-compliant systems impacting rights or safety.

Jurisdiction	Regulation	Compliance Date	Key Obligations
Federal Agencies	OMB M-24-10	December 1, 2024	Impact assessments, human oversight, independent evaluation
New York City	Local Law 144	July 5, 2023 (Active)	Bias audits for hiring AI, public disclosure
Colorado	AI Act SB24-205	June 30, 2026	Reasonable care, risk management, impact assessments

APAC Region

China: Interim Measures for Generative AI require lawful data sources, IP/PII compliance, content labeling, and security assessments for public-facing services.

India: Digital Personal Data Protection Act mandates lawful basis, consent management, breach notification, and Data Protection Impact Assessments for significant fiduciaries.

Singapore: Model AI Governance Framework provides nine governance dimensions including accountability, data governance, and incident reporting.

South Korea: AI Basic Act effective January 2026 establishes governance infrastructure, industry support, and safety requirements for high-risk AI.

2. Compliance Requirement Matrices

Core Governance Obligations

Requirement Category	EU AI Act	US Federal (M-24-10)	China GenAI	Priority Level
Governance Structure	Provider/Deployer obligations	CAIO appointment, AI Board	Provider cooperation duties	HIGH
Risk Assessment	Conformity assessment	Impact assessment required	Security assessment (public services)	HIGH
Documentation	Technical documentation	Annual certification	Algorithm filing	MEDIUM
Monitoring	Post-market monitoring	Periodic reviews	Content moderation	HIGH
Incident Reporting	15/2/10-day timeline	Stop-use for excessive risk	Cooperation with authorities	HIGH

Transparency and Notice Requirements

Use Case	Requirement	Jurisdiction	Timeline
General Purpose AI	Model transparency obligations	EU	August 2, 2025
Employment Decisions	Bias audit publication, candidate notice	NYC	Active (within 10 business days)
Generated Content	Deep-synthesis content labeling	China	Active
Rights-Impacting AI	Opt-out mechanisms where feasible	US Federal	December 1, 2024

3. Implementation Timeline Charts

Critical Compliance Deadlines

Date	Milestone	Jurisdiction
Dec 1, 2024	Federal AI safeguards deadline / Stop-use enforcement	US Federal
2025	AI Act prohibitions and literacy requirements	EU
Aug 2, 2025	General Purpose AI model obligations	EU
Jan 2026	AI Basic Act effective date	South Korea
Jun 30, 2026	Colorado AI Act compliance date	Colorado, US
Aug 2, 2026	AI Act general application	EU
2027	Article 6(1) risk-scoping provisions	EU

Phased Implementation Roadmap

Phase 1: Immediate (Next 30 Days)

- ☐ Establish AI Governance Board with clear decision rights
- ☐ Appoint Chief AI Officer and define roles/responsibilities
- ☐ Complete comprehensive AI system inventory
- ☐ Implement stop-use freeze for high-risk systems lacking safeguards
- ☐ Set up incident reporting channels with EU timing standards

Phase 2: Foundation (90 Days)

- ☐ Deploy NIST AI Risk Management Framework controls
- ☐ Implement bias audit processes for employment AI
- ☐ Establish content provenance pipeline for Generative AI
- ☐ Map high-risk use cases to regulatory categories
- ☐ Create vendor assessment and recertification program

Phase 3: Maturation (6-12 Months)

- ☐ EU AI Act readiness for high-risk and GPAI systems
- ☐ Colorado AI Act program implementation
- ☐ Sector-specific overlays (finance, healthcare, automotive)
- ☐ Third-party model governance and validation
- ☐ Continuous monitoring and improvement processes

4. Cost Impact Assessments

Implementation Budget Drivers

Cost Category	One-Time Investment	Annual Operating Cost	Key Components
Governance Infrastructure	$200K - $500K	$300K - $800K	CAIO office, governance board, policy development
Technology Platform	$150K - $400K	$100K - $300K	Model registry, monitoring tools, audit systems
Risk & Validation	$100K - $300K	$200K - $600K	Impact assessments, bias testing, validation processes
Legal & Compliance	$75K - $200K	$150K - $400K	Policy templates, training, regulatory monitoring
Training & Change Mgmt	$50K - $150K	$75K - $200K	Staff training, process adoption, communication

Penalty and Enforcement Costs

EU AI Act Penalties:

- Prohibited practices: Up to €35M or 7% of global annual turnover
- Operator obligations: Up to €15M or 3% of global annual turnover
- Information requirements: Up to €7.5M or 1% of global annual turnover

US Enforcement Examples:

- FTC Rite Aid settlement: 5-year facial recognition ban, mandatory deletion, independent assessments
- Federal stop-use orders for non-compliant systems impacting rights or safety
- Potential class action lawsuits for algorithmic bias in employment, lending, housing

ROI Considerations

- **Risk Mitigation:** Avoid regulatory penalties, reputational damage, litigation costs
- **Operational Efficiency:** Standardized processes, automated compliance checks

- **Competitive Advantage:** Trusted AI deployment, customer confidence, market access
- **Innovation Enablement:** Clear guardrails for safe AI experimentation and deployment

5. Vendor Evaluation Frameworks

RFP-Ready Assessment Criteria

Governance and Policy Capabilities

Criterion	Required	Preferred	Evaluation Weight
NIST AI RMF Mapping	✓	Full GOVERN/MAP/MEASURE/MANAGE lifecycle	25%
Multi-jurisdiction Support	US + EU	Global (US, EU, APAC)	20%
Policy Configuration	Basic templates	Configurable per use case/jurisdiction	15%
Evidence Generation	Audit reports	Regulator-ready documentation export	20%
Integration APIs	REST/GraphQL	Native ML platform integrations	20%

Model Lifecycle Management

- ☐ Comprehensive model registry with version control and lineage tracking
- ☐ Automated bias and fairness testing pipelines
- ☐ Red-teaming capabilities for Generative AI systems
- ☐ Explainability tools appropriate to model complexity and risk level
- ☐ Real-world performance monitoring with drift detection
- ☐ Deactivation and rollback capabilities with user communication plans

Incident Management and Reporting

- ☐ Configurable incident severity definitions and escalation workflows
- ☐ EU AI Act timeline compliance (15/2/10-day reporting windows)
- ☐ Automated report generation with regulatory routing
- ☐ Evidence capture and retention for investigations

- ☐ Corrective and Preventive Action (CAPA) workflow management

Privacy and Security Controls

- ☐ Data minimization enforcement and PII detection guardrails
- ☐ Privacy-Enhancing Technologies (PETs) support
- ☐ Automated breach notification workflows
- ☐ Supplier risk assessment and IP protection controls
- ☐ Content provenance and watermarking for Generative AI

Sector-Specific Requirements

Financial Services

- ☐ SR 11-7 validation workflow templates and challenger model frameworks
- ☐ Explainability reporting commensurate with decision materiality
- ☐ Backtesting and outcomes analysis capabilities
- ☐ Independent validation evidence and reviewer assignment
- ☐ ESMA MiFID II organizational controls for EU investment services

Healthcare and Life Sciences

- ☐ FDA Software as Medical Device (SaMD) change control planning
- ☐ Predetermined Change Control Plans (PCCP) for ML/AI modifications
- ☐ Real-world performance monitoring with clinical outcome tracking
- ☐ Patient-centric transparency and labeling capabilities
- ☐ Good Machine Learning Practice (GMLP) evidence generation

Automotive and Transportation

- ☐ UNECE R155 Cyber Security Management System (CSMS) integration
- ☐ Vehicle lifecycle security monitoring and threat analysis
- ☐ AI model telemetry aligned with automotive cybersecurity frameworks
- ☐ Over-the-air update validation and rollback capabilities

6. Audit Preparation Checklists

Universal AI Governance Audit Checklist

- ☐ Current AI system inventory with risk classifications and designated owners
- ☐ AI governance charter with defined roles, responsibilities, and decision rights
- ☐ Comprehensive model documentation (purpose, data sources, design assumptions, limitations)
- ☐ Testing, Evaluation, Verification, and Validation (TEVV) results and reports
- ☐ Human oversight and human-in-the-loop configuration documentation
- ☐ Incident response standard operating procedures and escalation matrices
- ☐ Last 12 months of monitoring logs and performance metrics
- ☐ Model decommissioning and retirement plans
- ☐ Third-party vendor assessments and contractual safeguards
- ☐ Staff training records and competency certifications

EU AI Act Specific Requirements

- ☐ Technical documentation package for high-risk AI systems
- ☐ Conformity assessment evidence and CE marking documentation
- ☐ Post-market monitoring plan and implementation evidence
- ☐ Serious incident reporting procedures and historical incident logs
- ☐ Transparency measures and user notification processes
- ☐ Data governance attestations and supplier IP compliance
- ☐ General Purpose AI model obligations compliance (if applicable)
- ☐ Quality management system documentation and audit trail

US Federal (OMB M-24-10) Requirements

- ☐ Chief AI Officer appointment documentation and governance structure
- ☐ Completed impact assessments for rights and safety-impacting AI
- ☐ Real-world testing logs and validation methodologies

- ☐ Independent evaluation reports from qualified third parties
- ☐ Discrimination analysis and mitigation strategies for rights-impacting AI
- ☐ Opt-out process implementation (where feasible for rights-impacting AI)
- ☐ Annual certification submissions and waiver documentation
- ☐ Public AI inventory entries and transparency reporting
- ☐ Stop-use decision documentation and remediation evidence

NYC Employment AI (Local Law 144)

- ☐ Annual bias audit report with statistical analysis methodology
- ☐ Published bias audit summary accessible to candidates
- ☐ Candidate notification process (10 business days advance notice)
- ☐ Automated Employment Decision Tool (AEDT) scope and usage documentation
- ☐ Historical audit results and year-over-year bias trend analysis
- ☐ Vendor bias audit attestations and third-party validation

Financial Services (SR 11-7/OCC Model Risk Management)

- ☐ Model development documentation demonstrating conceptual soundness
- ☐ Independent model validation reports and validator qualification evidence
- ☐ Ongoing monitoring procedures and model performance tracking
- ☐ Explainability assessment appropriate to model risk and complexity
- ☐ Bias evaluation methodology and demographic impact analysis
- ☐ Third-party model due diligence and vendor management controls
- ☐ Model inventory with risk ratings and validation frequencies
- ☐ Challenger model development and benchmarking results

APAC Privacy and Safety Requirements

China Generative AI Compliance

- ☐ Lawful training data source attestations and intellectual property compliance
- ☐ Personal information processing consent and rights management

- ☐ Deep-synthesis content labeling implementation and audit trail
- ☐ Algorithm registration and security assessment documentation (if required)
- ☐ Content moderation policies aligned with national standards
- ☐ User complaint handling and government cooperation procedures

India DPDP Act Compliance

- ☐ Lawful basis documentation and consent management records
- ☐ Data protection notice delivery and user acknowledgment logs
- ☐ Personal data breach notification procedures and Board correspondence
- ☐ Data Protection Impact Assessment (DPIA) for significant fiduciaries
- ☐ Data Protection Officer appointment and auditor designation (if applicable)
- ☐ Children's consent verification mechanisms and parental controls
- ☐ Cross-border data transfer safeguards and adequacy assessments

7. Risk Mitigation Strategies

Shift-Left Risk Management

Strategy: Embed risk controls early in the AI development lifecycle using the NIST AI Risk Management Framework's GOVERN and MAP functions.

Implementation Tactics

- **Risk-Tied Acceptance Criteria:** Require documented risk assessments and mitigation plans in every model development milestone
- **Automated Gates:** Block production deployment without completed TEVV artifacts, impact assessments, and approval workflows
- **Design-Time Controls:** Implement bias detection, fairness constraints, and explainability requirements during model training
- **Data Governance:** Enforce data quality, lineage, and privacy controls at ingestion rather than post-processing

Generative AI Specific Controls

Challenge: Generative AI systems present unique risks including content authenticity, prompt injection, and uncontrolled generation.

Mandatory Safeguards

- ☐ Content provenance and watermarking implementation where technically feasible
- ☐ Red-team testing for jailbreaks, prompt injection, and safety guardrail bypass
- ☐ Personal Identifiable Information (PII) leakage detection and prevention
- ☐ Output filtering for harmful, biased, or inappropriate content generation
- ☐ User notification and labeling for AI-generated content
- ☐ Emergency deactivation procedures with user communication plans

Stop-Use Decision Framework

Trigger Conditions: Mirror US federal M-24-10 guidance for consistent enterprise-wide risk management.

Risk Level	Trigger Conditions	Required Actions	Timeline
Critical	Imminent harm to individuals, discrimination cannot be mitigated	Immediate stop-use, incident report, remediation plan	24 hours
High	Significant bias detected, performance below acceptable thresholds	Usage restrictions, enhanced monitoring, mitigation implementation	72 hours
Medium	Model drift, minor bias, documentation gaps	Corrective action plan, increased validation frequency	30 days

Third-Party Model Governance

Risk: Limited visibility and control over vendor-provided AI models and services.

Contractual Safeguards

- ☐ Service Level Agreements (SLAs) on model performance, bias metrics, and availability
- ☐ Intellectual property provenance warranties and indemnification clauses
- ☐ Data rights and usage restrictions with audit and deletion capabilities
- ☐ Security posture requirements including encryption, access controls, and incident response
- ☐ Evaluation transparency including test datasets, methodologies, and limitation disclosures
- ☐ Change notification requirements for model updates, retraining, or architecture modifications

Ongoing Validation Requirements

- ☐ Independent validation and recertification on defined schedules (annually minimum for high-risk)
- ☐ Continuous performance monitoring with vendor-provided APIs and telemetry
- ☐ Regular bias audits using organization-specific datasets and use cases
- ☐ Vendor security assessments and compliance certifications review
- ☐ Disaster recovery and business continuity plan validation

Financial Services

- **Explainability Standard:** Implement graduated explainability requirements based on decision materiality and customer impact
- **Model Validation:** Enforce SR 11-7 independent validation with qualified validators separate from development teams
- **Challenger Models:** Develop alternative approaches for critical decisions to validate primary model outcomes
- **Stress Testing:** Include AI models in enterprise stress testing scenarios and capital adequacy assessments

Healthcare and Life Sciences

- **Post-Market Monitoring:** Implement real-world performance tracking with clinical outcome correlation
- **Change Control:** Establish predetermined change control plans for FDA Software as Medical Device compliance
- **Patient Safety:** Prioritize safety monitoring with rapid response protocols for adverse events
- **Clinical Validation:** Require clinical evidence for medical AI deployments beyond technical validation

Automotive and Transportation

- **Safety Integration:** Align AI governance with existing functional safety standards (ISO 26262)
- **Cybersecurity Alignment:** Integrate with UNECE R155 Cyber Security Management Systems
- **Over-the-Air Updates:** Implement secure update validation and rollback capabilities
- **Edge Deployment:** Address unique challenges of AI inference in resource-constrained vehicle environments

8. Policy Template Libraries

AI Governance Charter Template

Executive Summary

This charter establishes the organizational framework for responsible AI development, deployment, and governance across [Organization Name]. It defines roles, responsibilities, decision rights, and accountability mechanisms to ensure compliance with applicable regulations and ethical AI principles.

Governance Structure

Role	Responsibilities	Decision Authority
Chief AI Officer (CAIO)	Strategic oversight, regulatory compliance, cross-functional coordination	AI strategy, policy approval, resource allocation
AI Governance Board	Policy review, risk assessment, incident escalation	Stop-use decisions, risk tolerance, audit findings
Model Owners	Lifecycle management, documentation, performance monitoring	Day-to-day operations, user access, minor updates
Independent Validators	Third-party assessment, bias evaluation, performance testing	Validation approval, recommendation for deployment

Model Lifecycle Management Policy

Development Phase Requirements

- ☐ AI system registration in enterprise model registry with unique identifier
- ☐ Risk classification using [EU AI Act / NIST AI RMF / Internal] taxonomy
- ☐ Impact assessment completion for rights and safety-impacting systems
- ☐ Data governance plan with lineage, quality, and privacy controls
- ☐ Bias and fairness evaluation using approved methodologies and metrics
- ☐ Documentation package including purpose, assumptions, limitations, and usage guidelines

Validation and Testing Gates

- ☐ Technical validation including accuracy, robustness, and performance benchmarks
- ☐ Independent validation by qualified third-party for high-risk systems
- ☐ Red-team testing for Generative AI including prompt injection and safety guardrails
- ☐ Real-world testing with representative data and user scenarios
- ☐ Explainability assessment appropriate to system complexity and risk level
- ☐ Security assessment including adversarial robustness and data protection

Deployment and Monitoring

- ☐ Human oversight configuration with appropriate level of human involvement
- ☐ Performance monitoring dashboard with key metrics and alert thresholds
- ☐ Incident detection and reporting procedures with defined escalation paths
- ☐ User training and communication plan including AI transparency notices
- ☐ Periodic review schedule based on risk classification and regulatory requirements
- ☐ Change control procedures for model updates, retraining, and parameter modifications

Generative AI Safety Policy Template

Content Generation Controls

- ☐ Input validation and sanitization to prevent prompt injection attacks
- ☐ Output filtering for harmful, biased, inappropriate, or illegal content
- ☐ Content provenance implementation using watermarking or metadata where feasible
- ☐ User notification requirements for AI-generated content
- ☐ Rate limiting and usage monitoring to prevent abuse
- ☐ Emergency content removal and system deactivation procedures

Data and Privacy Protection

- ☐ Training data validation for lawful acquisition and intellectual property compliance

- ☐ Personal information detection and handling procedures
- ☐ Data minimization enforcement in training and inference
- ☐ Cross-border data transfer controls and localization requirements
- ☐ User data retention and deletion policies
- ☐ Third-party data sharing restrictions and contractual safeguards

Incident Response Standard Operating Procedure

Incident Classification Matrix

Severity Level	Definition	Response Time	Notification Requirements
Critical (P0)	Imminent harm, widespread impact, regulatory violation	15 minutes	CAIO, Legal, Regulators (2-15 days per jurisdiction)
High (P1)	Significant bias, performance degradation, security breach	2 hours	Model owner, AI Governance Board
Medium (P2)	Minor bias, documentation gaps, user complaints	24 hours	Model owner, relevant stakeholders

Response Procedures

1. **Detection and Assessment:** Automated monitoring alerts or manual reporting triggers incident classification
2. **Initial Response:** Immediate containment actions including stop-use decisions if warranted
3. **Investigation:** Root cause analysis, impact assessment, and evidence collection
4. **Notification:** Internal stakeholders, affected users, and regulatory bodies per timeline requirements
5. **Remediation:** Corrective actions, system modifications, and preventive measures
6. **Documentation:** Incident report, lessons learned, and process improvements

Employment AI Policy (NYC Local Law 144 Compliance)

Automated Employment Decision Tool (AEDT) Definition

Any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation, that is used to substantially assist or replace discretionary decision making for employment decisions that impact natural persons.

Bias Audit Requirements

- ☐ Annual bias audit conducted by independent third party using NYC DCWP methodology
- ☐ Statistical analysis of selection rates and impact ratios by protected characteristics
- ☐ Publication of bias audit summary on company website accessible to candidates
- ☐ Retention of detailed audit reports for regulatory inspection
- ☐ Remediation plan development for identified bias above acceptable thresholds

Candidate Notification Process

- ☐ Notice provided at least 10 business days before AEDT use in selection process
- ☐ Information about job requirements and selection criteria used by AEDT
- ☐ Instructions for requesting reasonable accommodation or alternative selection process
- ☐ Contact information for inquiries about AEDT use and bias audit results

9. Compliance Roadmaps

30-Day Critical Path Implementation

Week 1: Governance Foundation

Action Item	Owner	Deliverable	Success Criteria
Appoint Chief AI Officer	CEO/Board	CAIO appointment letter, role definition	Named individual with defined authority
Form AI Governance Board	CAIO	Charter, member appointments, meeting cadence	Cross-functional board with decision rights
Emergency AI inventory	IT/Engineering	Comprehensive system catalog with risk flags	100% coverage of production AI systems

Week 2-3: Risk Assessment and Controls

Action Item	Owner	Deliverable	Success Criteria
High-risk system identification	CAIO/Risk	Risk classification matrix, system categorization	EU AI Act and US M-24-10 mapping complete
Stop-use assessment	Model Owners	Impact assessments for rights/safety systems	Go/no-go decision for each high-risk system
Incident reporting setup	Operations	Incident classification, escalation procedures	15/2/10-day EU timeline capability

Week 4: Documentation and Communication

Action Item	Owner	Deliverable	Success Criteria
Policy framework adoption	Legal/CAIO	AI governance charter, lifecycle policy	Board-approved policies in effect
Staff communication	HR/Communications	All-hands announcement, training schedule	100% staff awareness of new governance
Vendor notifications	Procurement	Contract review, compliance requirements	All AI vendors notified of new standards

90-Day Foundation Building

NIST AI RMF Implementation

- ☐ **GOVERN:** Establish AI governance structure, policies, and accountability mechanisms
- ☐ **MAP:** Complete AI system inventory with comprehensive risk mapping and context analysis
- ☐ **MEASURE:** Deploy testing, evaluation, verification, and validation (TEVV) processes
- ☐ **MANAGE:** Implement ongoing monitoring, incident response, and continuous improvement

Jurisdiction-Specific Compliance

Jurisdiction	Priority Actions	Timeline	Key Deliverables
US Federal	M-24-10 safeguards implementation	Complete by Dec 1, 2024	Impact assessments, independent evaluations, annual certifications
NYC Employment	AEDT bias audit process	Immediate if using hiring AI	Annual audit, public summary, candidate notice process
EU High-Risk	AI Act readiness assessment	Target Aug 2026	Technical documentation, conformity assessment preparation
China GenAI	Generative AI Measures compliance	Immediate for public services	Data source validation, content labeling, security assessment

6-12 Month Maturation Phase

Advanced Governance Capabilities

- ☐ Automated compliance monitoring with real-time dashboards and alerting
- ☐ Advanced bias detection and mitigation across protected characteristics
- ☐ Comprehensive third-party model validation and certification program
- ☐ Integration with enterprise GRC platforms and regulatory reporting systems
- ☐ Sector-specific overlays for finance, healthcare, automotive, and other regulated industries

Continuous Improvement Framework

- ☐ Quarterly governance effectiveness reviews with stakeholder feedback
- ☐ Annual policy updates incorporating regulatory changes and lessons learned
- ☐ Benchmarking against industry best practices and peer organizations
- ☐ Regular training updates and competency assessments for staff
- ☐ Vendor ecosystem management and performance optimization

10. Enforcement Mechanisms and Penalties

European Union Enforcement

Administrative Fines Structure

Violation Category	Maximum Fine	Example Violations	Enforcement Authority
Prohibited AI Practices	€35M or 7% global turnover	Subliminal techniques, social scoring, real-time biometric ID	National competent authorities
Operator Obligations	€15M or 3% global turnover	High-risk system non-compliance, inadequate human oversight	National competent authorities
Information Requirements	€7.5M or 1% global turnover	Misleading information, documentation failures	National competent authorities

SME Protection: Small and medium enterprises receive the lower of the percentage or absolute amount, providing some protection from disproportionate penalties.

Enforcement Process

1. **Investigation:** National authorities conduct investigations based on complaints, market surveillance, or own initiative
2. **Corrective Measures:** Authorities may require immediate corrective actions or temporary restrictions
3. **Administrative Sanctions:** Formal penalties imposed following due process and right of defense
4. **Public Disclosure:** Significant violations and penalties may be publicly disclosed
5. **Appeals Process:** Right to judicial review of administrative decisions and penalties

United States Enforcement Landscape

Federal Agency Enforcement (M-24-10)

- **Stop-Use Orders:** Mandatory discontinuation of AI systems failing to meet minimum safeguards by December 1, 2024

- **Budget Impact:** Non-compliant agencies risk budget restrictions and oversight escalation
- **Personnel Action:** Individual accountability for Chief AI Officers and senior officials
- **Public Transparency:** Mandatory public disclosure through AI inventory reporting

Federal Trade Commission (FTC) Precedents

Rite Aid Settlement Example (December 2023):

- Five-year ban on facial recognition technology use for surveillance
- Mandatory deletion of existing facial recognition databases and related algorithms
- Independent third-party assessments of any future facial recognition implementations
- Comprehensive employee training on algorithmic bias and privacy protection
- CEO certification requirements for compliance with settlement terms
- Enhanced data security and governance program implementation

State and Local Enforcement

Jurisdiction	Enforcement Mechanism	Penalty Structure	Notable Features
Colorado	Attorney General exclusive enforcement	Civil penalties, injunctive relief	Private right of action explicitly excluded
New York City	Department of Consumer and Worker Protection	Fines up to $500 first violation, $1,500 subsequent	Public disclosure of violations
California (proposed)	Civil penalties, regulatory enforcement	Varies by specific legislation	Multiple bills under consideration

APAC Enforcement Approaches

China Regulatory Enforcement

- **Administrative Penalties:** Fines, suspension of services, and license revocation for non-compliance

- **Criminal Liability:** Potential criminal charges for severe violations involving national security or public safety
- **Social Credit Impact:** Violations may impact corporate social credit scores and business operations
- **Industry Cooperation:** Mandatory cooperation with government investigations and security assessments

India DPDP Act Enforcement

- **Data Protection Board:** Specialized authority with investigation and penalty powers
- **Financial Penalties:** Up to ₹500 crores (approximately $60M USD) for significant violations
- **Corrective Measures:** Mandatory remediation, system improvements, and process changes
- **Business Restrictions:** Potential suspension of data processing activities

Singapore Soft Law Approach

- **Voluntary Framework:** Model AI Governance Framework provides guidance rather than mandatory requirements
- **Industry Adoption:** Used by organizations for self-assessment and by regulators for evaluation
- **Regulatory Expectations:** Compliance with framework becomes regulatory expectation in practice
- **Sectoral Enforcement:** Sector-specific regulators may incorporate AI governance requirements

Private Litigation Risks

Common Legal Theories

- **Discrimination Claims:** Civil rights violations in employment, housing, lending, and public accommodations
- **Privacy Torts:** Invasion of privacy, unauthorized data use, and biometric information violations

- **Consumer Protection:** Deceptive practices, unfair business practices, and false advertising
- **Negligence:** Failure to exercise reasonable care in AI system design, testing, and deployment
- **Contract Claims:** Breach of terms of service, privacy policies, and vendor agreements

Damage Categories

- **Compensatory Damages:** Actual financial losses, emotional distress, and opportunity costs
- **Statutory Damages:** Predetermined amounts under specific privacy and civil rights statutes
- **Punitive Damages:** Additional penalties for willful or grossly negligent conduct
- **Injunctive Relief:** Court orders requiring changes to AI systems or business practices
- **Attorney Fees:** Potential fee-shifting to defendants in civil rights and consumer protection cases

11. Sector-Specific Requirements

Financial Services

US Banking Regulatory Framework

SR 11-7 Model Risk Management Guidance (Federal Reserve): Establishes comprehensive requirements for model development, validation, and governance in banking organizations.

Core Requirements

Component	Requirement	Implementation Standard
Model Development	Conceptual soundness with documented methodology	Clear model purpose, assumptions, limitations, and appropriate data
Independent Validation	Third-party assessment separate from development	Qualified validators, comprehensive testing, challenger models
Ongoing Monitoring	Performance tracking and model risk assessment	Key metrics, thresholds, periodic validation, backtesting
Governance Structure	Board oversight and senior management accountability	Model inventory, risk rating, approval authority, reporting

OCC Model Risk Management Handbook Specifics

- ☐ Explainability requirements proportionate to model complexity and business impact
- ☐ Bias evaluation across demographic groups and protected characteristics
- ☐ Third-party model due diligence including vendor management and validation
- ☐ Model change management with version control and impact assessment
- ☐ Documentation standards supporting regulatory examination and audit

EU Investment Services (ESMA Guidance)

MiFID II AI Requirements: ESMA provides specific guidance on AI use in investment services to retail clients, emphasizing organizational requirements and best

interest obligations.

- ☐ Organizational controls ensuring appropriate AI system design and operation
- ☐ Staff competency requirements and ongoing training on AI systems
- ☐ Client best interest analysis considering AI-driven recommendations
- ☐ Bias and opacity risk management with appropriate disclosure
- ☐ Governance arrangements ensuring senior management oversight

Healthcare and Life Sciences

FDA Software as Medical Device (SaMD) Framework

AI/ML Action Plan: FDA's comprehensive approach to regulating AI and machine learning in medical devices with emphasis on total product lifecycle and adaptive systems.

Key Regulatory Pathways

Device Category	Regulatory Pathway	Key Requirements
AI/ML-Enabled Device	510(k) or PMA	Traditional medical device requirements plus AI-specific considerations
Adaptive AI/ML Device	Predetermined Change Control Plans	FDA pre-authorization for specific types of modifications
Continuously Learning	Good Machine Learning Practice	Enhanced monitoring, validation, and post-market surveillance

Implementation Requirements

- ☐ **Algorithm Change Protocol:** Predetermined Change Control Plans (PCCP) for FDA-authorized modifications
- ☐ **Real-World Performance Monitoring:** Post-market surveillance with clinical outcome tracking
- ☐ **Transparency and Usability:** User-centered design with appropriate clinical decision support

- ☐ **Quality Management Integration:** AI/ML considerations in ISO 13485 quality systems
- ☐ **Clinical Evidence Generation:** Appropriate clinical validation beyond technical performance

EU Medical Device Regulation (MDR) AI Considerations

- ☐ Classification rules considering AI/ML complexity and risk level
- ☐ Clinical evaluation requirements with post-market clinical follow-up
- ☐ Notified body involvement for higher-risk AI medical devices
- ☐ Unique Device Identification (UDI) and traceability requirements
- ☐ Post-market surveillance and vigilance reporting integration

Automotive and Transportation

UNECE Regulation No. 155 - Cyber Security Management System

Cybersecurity Framework: Mandatory cybersecurity management system for connected vehicles, providing structure for integrating AI governance with automotive cybersecurity.

CSMS Core Elements

Component	Requirement	AI Integration Considerations
Risk Assessment	Identification and analysis of cybersecurity risks	AI model vulnerabilities, adversarial attacks, data poisoning
Risk Treatment	Implementation of appropriate security measures	AI model protection, secure inference, update validation
Monitoring		