The Verapath Artificial Intelligence Regulatory Roundup

Mythos changes everything

May 2026

Alec Crawford, Verapath Founder & CEO, aleccrawford@verapath.com
Ben Perl, Research Associate, benperl@verapath.com

Welcome to the first publication of Verapath's Regulatory Roundup. If you're a US financial services executive, risk leader, or compliance officer, this newsletter exists to save you time. Each quarter, we cut through the noise of federal guidance, state legislation, and evolving supervisory expectations around AI to deliver what matters most: what's new, what it means for your institution, and what you need to do about it.

We've structured every section around a consistent format (context, what happened, implications, and concrete action items) so you can scan quickly and go deep where it counts. Our goal is to help you move from awareness to preparedness, whether it's an SEC stance on "AI washing," a new state transparency mandate, or the emergence of the financial sector's first industry-driven AI risk management framework.

The current US administration has encouraged the use of AI. It appeared that regulation and enforcement across industries was less onerous than the prior administration. Then...Mythos happened. The administration, starting with the Secretary of the Treasury, Scott Bessent, has become very concerned about the deleterious effect of advanced AI on cybersecurity, and by extension the banking system and other regulated financials. Be prepared.

The Verapath software facilitates compliance with rules and regulations for AI and data privacy, including full audit trails and a built-in e-discovery tool. We also have developed a CRI AI RMF 1.0 compliance wizard and reporting tool. Please contact the author for more information or a demo.

Table of Contents

---

1. What You Need to Know

The CRI Financial Services AI Risk Management Framework (FS AI RMF), released February 2026 with FDIC and U.S. Treasury backing, provides 230 control objectives mapped to NIST's AI RMF.[1,2]

Colorado's AI Act (SB 24-205) takes effect June 30, 2026, and explicitly provides a safe harbor for institutions that adopt the NIST AI RMF or ISO/IEC 42001. Regulated banks and credit unions subject to federal prudential oversight may qualify for a separate exemption.[3,4]

New York's RAISE Act, signed December 19, 2025, and effective January 1, 2027, targets large frontier AI model developers, not deployers, but financial institutions using covered models should monitor compliance obligations and vendor contract implications.[5,6]

Michigan's DIFS Bulletin 2026-03 (effective January 14, 2026) requires a written AI Systems Program for all state-regulated financial service providers. It references NIST's AI RMF as an appropriate framework but does not provide a formal safe harbor.[7,8,9]

The SEC's 2026 Exam Priorities embed AI governance across all major categories, from accurate disclosures and anti-"AI washing" to cybersecurity integration and Regulation S-P compliance (June 3, 2026 for small RIAs).[10]

Multi-state institutions face overlapping and sometimes conflicting requirements. Adopting the CRI FS AI RMF is currently the strongest single strategy for demonstrating compliance across jurisdictions.[11]

---

2. Federal Regulatory News: AI & Financial Institutions

2a. NIST AI RMF and the CRI FS AI RMF: The Foundation and the Building Code

THE ANALOGY: Think of NIST as the architectural blueprint: it defines the rooms (Govern, Map, Measure, Manage) and what each room is for. The CRI FS AI RMF is the building code for financial services: it tells you exactly what materials to use, what inspections to pass, and what documentation the examiner will want to see. All while keeping the same room layout.

NIST AI RMF: The Foundation

Context: Released January 26, 2023, the NIST AI Risk Management Framework is a voluntary, sector-agnostic, and use-case-agnostic framework designed to help organizations incorporate trustworthiness into the design, development, use, and evaluation of AI systems. It provides a flexible baseline that any organization can adapt to any industry.[12]

What: The framework is organized around four core functions (Govern, Map, Measure, and Manage) broken into categories and subcategories. Govern applies across all stages of an organization's AI risk management processes, while Map, Measure, and Manage can be applied in system-specific contexts and at specific stages of the AI lifecycle. NIST provides principles and outcomes but deliberately leaves implementation details to each organization.[12]

Implication: For financial institutions, NIST's generality is both its strength and its limitation. It establishes the vocabulary and conceptual structure that regulators, auditors, and industry bodies increasingly reference, but it lacks the prescriptive, sector-specific controls that examiners expect to see. Applying NIST's general framework to the operations of financial institutions leaves

significant gaps around fair lending, model validation under SR 11-7, consumer protection, and third-party vendor oversight.[13,14]

CRI FS AI RMF: The Financial Services Layer

Context: On February 12, 2026, the Cyber Risk Institute officially launched the FS AI RMF, developed collaboratively by 108 financial institutions working through CRI and the Financial Services Sector Coordinating Council (FSSCC). This framework emerged from industry consensus, not regulatory mandate. The U.S. Treasury then formally released the framework alongside its AI Lexicon on February 19, 2026, giving the FS AI RMF quasi-official status.[1,2,15]

What: The FS AI RMF is structurally aligned with NIST's four-function model (Govern, Map, Measure, Manage) but expands it with 230 control objectives organized across a detailed Risk and Control Matrix. Every FS AI RMF control maps back to a NIST AI RMF subcategory, ensuring compatibility while adding financial-sector specificity.[11,14,15,16]

Where the CRI FS AI RMF Expands Beyond NIST

Dimension	NIST AI RMF	CRI FS AI RMF
Specificity	General outcomes and principles	230 prescriptive control objectives covering governance, data, model development, validation, monitoring, third-party risk, and consumer protection
Maturity Model	Not addressed	AI Adoption Stage Questionnaire with four stages (Initial, Minimal, Evolving, Embedded)
Governance	General governance guidance	Board-level AI committees, SR 11-7 integration, explicit risk appetite statements for AI-driven decisions
Bias & Fairness	General fairness principles	Bias testing against protected classes under fair lending laws; model validation meeting OCC and FFIEC standards
Evidence Requirements	Not specified	Examination-ready evidence: logged artifacts tied to specific control objectives, traceable from policy to control to test to documentation

Dimension	NIST AI RMF	CRI FS AI RMF
Third-Party Risk	Basic supply chain considerations	Requires evaluation of vendor AI model performance, bias characteristics, hallucination rates, and security posture
Cross-Regulatory Mapping	Not addressed	Maps to 15+ frameworks including EU AI Act, ISO 42001, SR 11-7, FFIEC/OCC guidance, and CFPB requirements

Implication: The FS AI RMF is positioned to become the de facto reference for risk managers, auditors, and regulators examining AI practices in financial services. Institutions that adopt this framework will be better prepared for regulatory examinations and will generate compliance evidence that maps across multiple regulatory bodies simultaneously.[14]

Action Items:

1. Download and review the CRI FS AI RMF and its companion materials (Risk and Control Matrix, Evidence Guide, Adoption Stage Questionnaire) from cyberriskinstitute.org.[1]
2. Complete the AI Adoption Stage Questionnaire to benchmark your institution's current maturity and identify applicable control objectives.[16]
3. Map your existing AI governance controls to the FS AI RMF's 230 control objectives and conduct a gap analysis.
4. Use the framework's cross-regulatory mapping to consolidate compliance evidence across SEC, OCC, FFIEC, and state-level requirements.
5. Verapath can massively reduce your compliance burden. Our software ingests your policies and procedures, incorporates items that the Verapath software facilitates compliance with and produces a full compliance report at the touch of a button. More than half of the FS AI RMF's control objectives can be automated through purpose-built AI risk management tooling. The rest can be completed using our automated compliance wizard.

2b. U.S. Department of the Treasury: New AI Resources

1. AI Lexicon

What: A standardized set of terms and definitions for artificial intelligence, risk categories, and capabilities in the context of financial services.[2]

Implication: Enables regulators, financial institutions, and vendors to use consistent language when discussing AI systems and risks. This reduces translation friction across legal, risk, engineering, and business functions.[2,14]

2. FS AI RMF Partnership

What: Treasury's formal release of the CRI-developed FS AI RMF adapts the NIST AI RMF for the unique regulatory expectations of the financial sector, providing practical tools for evaluating, documenting, and managing AI risks throughout the AI system lifecycle.[2]

Implication: Treasury's endorsement signals that the FS AI RMF is not merely industry guidance. It is the operational architecture standard that examiners will increasingly reference. Institutions should treat adoption not as optional best practice but as a baseline expectation.[14]

Action Items:

1. Integrate Treasury's AI Lexicon into your internal policies, training materials, and documentation to ensure consistent terminology across teams.
2. Use the lexicon definitions in regulatory filings and disclosures, ensuring alignment with Treasury and peer institutions.
3. Assess current AI risk management practices against the FS AI RMF; identify gaps in governance, testing, bias controls, and consumer protection.
4. Train risk, compliance, IT, and business teams on the FS AI RMF, ensuring readiness for regulatory audits and cross-agency inquiries.

2c. SEC: AI Governance, Cybersecurity, and Regulation S-P

1. AI Governance and Accurate Disclosures Are Top Priorities

Context: The SEC's Division of Examinations' 2026 exam priorities highlight a sharp focus on emerging technologies, especially artificial intelligence.[10]

What: For SEC-regulated financial companies, this means ensuring that all client communications, Form ADV disclosures, and marketing materials accurately represent the extent and role of AI in your processes. The SEC specifically warns against "AI washing", making claims about AI capabilities that aren't substantiated. Human oversight remains essential for all material AI-driven decisions.[10]

Action: Conduct a targeted review of all public and client-facing documents for accurate, non-exaggerated descriptions of AI usage. Maintain records of how and why AI tools are chosen and used in your workflows.

2. Cybersecurity and AI Risk Management Are Now Inseparable

Context: The SEC expects SEC-regulated financial companies to integrate AI into their existing cybersecurity frameworks and operational resiliency programs.[10]

What: Expectations include addressing AI-enabled risks (deepfakes, AI-powered phishing, polymorphic malware) within your information security policies; reviewing how AI is used both internally and by third-party vendors; and ensuring your cybersecurity incident response plan explicitly addresses AI-related threats. This must be harmonized with Regulation S-P amendments.[17]

Action: Update cybersecurity training, access controls, and vendor oversight to specifically identify and address AI-related threats.

3. Continuous Supervision, Testing, and Documentation

What: AI is no longer treated as a niche topic. It is now embedded in nearly all key SEC exam categories. SEC-regulated financial companies must demonstrate ongoing monitoring, testing, and supervision of AI models, including how outputs are validated for accuracy, freedom from bias, and compliance with fiduciary obligations.[10]

Action: Enhance documentation of your AI risk assessment and mitigation efforts. Maintain clear records of model validation, oversight protocols, and how AI-related incidents are handled.

4. Regulation S-P: AI and Data Governance Convergence

Context: Recent amendments to Regulation S-P (adopted 2024, phased compliance by December 3, 2025 for large firms and June 3, 2026 for every firm) bring new cyber-focused obligations that directly affect AI governance and data protection.[17]

What: RIAs must have comprehensive written policies addressing safeguarding and disposal of customer data, incident response, notification procedures, and oversight of service providers, including those that use AI. AI-related data flows are explicitly in scope.[17]

Action: Conduct a gap analysis of your compliance program against the SEC's 2026 exam priorities and Regulation S-P amendments.

SEC Summary at a Glance

Priority Area	SEC Focus	Action Required
AI Governance & Disclosures	No AI washing; accurate, substantiated claims	Review and enhance all public and client-facing materials

Priority Area	SEC Focus	Action Required
Cybersecurity & AI Risk	Integrate AI into cyber policies; address AI-enabled threats	Update training, controls, and vendor oversight programs
Supervision & Documentation	Evidence of continuous AI oversight, testing, and incident handling	Enhance documentation and annual compliance reviews
Reg S-P & Data Governance	Comprehensive customer data and AI risk policies	Conduct gap analysis; update cybersecurity program

---

2d. The White House: National AI Policy Framework

Executive Order: Ensuring a National Policy Framework for AI

Context: This Executive Order, signed December 11, 2025, arrives as states like California, Colorado, and New York enact comprehensive and sometimes divergent AI regulations.[18]

What: The Order establishes a coordinated national policy framework for AI. It directs the FTC to issue guidance on applying unfairness and deception standards to AI technologies. The DOJ's AI Litigation Task Force is authorized to challenge state laws deemed to conflict with a "minimally burdensome national standard."[18,19]

Implication: This represents a White House-led attempt to limit or override state-level AI regulations in favor of federal preemption. However, until preemption is enacted or successfully litigated, state laws remain enforceable.[18]

Legislative Follow-Up: National Policy Recommendations (March 2026)

Context: Following the Executive Order, the White House released detailed legislative recommendations to Congress covering child safety, community protection, intellectual property, free speech, workforce readiness, and federal preemption.[20]

What: Key proposals include mandating robust AI platform protections for minors; protecting digital likeness and voice from unauthorized AI use; launching regulatory sandboxes; expanding AI education programs; and establishing a national AI standard to override conflicting state AI laws while preserving state authority over core consumer and public safety issues.[20]

Implication: If enacted, these recommendations would replace most state-level AI rules with a uniform national standard, streamlining compliance for financial institutions but introducing a transition period with ongoing legal uncertainty.[20]

Action Items:

1. Monitor federal rulemaking and FTC guidance to anticipate new compliance requirements.
2. Prepare for continued multi-level compliance: until preemption is resolved, ensure adherence to both federal directives and the most stringent applicable state laws.
3. Engage with industry associations and advocacy groups to inform the regulatory process.
4. Update board and executive risk assessments to reflect the evolving federal-state regulatory dynamic.
5. Be ready to adapt compliance programs quickly as the scope of federal preemption is clarified.

---

3. State Regulatory Developments

The sections below analyze each state's AI legislation through a critical lens: how does each law relate to the NIST AI RMF and the CRI FS AI RMF? Where does it overlap, defer, or go beyond federal frameworks?

3a. At a Glance: State AI Regulation and NIST/CRI AI RMF 1.0 Alignment

Jurisdiction	Type	NIST/ CRI AI RMF 1.0 Relationship	Effective Date	Key Differentiator
Colorado (SB 24-205)	Comprehensive statute	Explicit safe harbor: rebuttable presumption for NIST/ISO 42001. Separate exemption for federally supervised banks.	June 30, 2026 (since delayed)	Only state with formal NIST-based affirmative defense
New York (RAISE Act)	Frontier model developer law	No direct safe harbor, but regulators may deem federal standards equivalent. Oversight within DFS.	January 1, 2027	Targets developers, not deployers. DFS enforcement intensity.
California (CCPA / SB-53 / AB 2013)	Layered statutes	No explicit NIST safe harbor. CRI/NIST supports but doesn't fully satisfy CA transparency mandates.	Various (in effect / phased)	AB 2013 training data transparency goes beyond any federal framework.
Michigan (Bulletin 2026-03)	Regulatory bulletin	References NIST AI RMF but no formal safe harbor.	Jan 14, 2026 (immediate)	Not a new law—enforcement signal. Written AIS Program required now.

CROSS-JURISDICTIONAL NOTE: Most state AI laws apply based on where the consumer or transaction is located, not where the institution is headquartered. Multi-state institutions should map their AI systems against each state's requirements based on their customer footprint, not just their domicile.

3b. Colorado: Artificial Intelligence Act (SB 24-205)

Context: Colorado's AI Act, signed May 2024, was set to take effect June 30, 2026 (already delayed from February 1, 2026). However, as of late April 2026, the law's enforcement is on hold. On April 27, 2026, a federal court paused enforcement while litigation challenging the law's constitutionality plays out. Separately, the Colorado legislature is actively considering SB-189, a bill that would repeal and substantially rewrite the law, replacing its core framework with narrower requirements. The legislature's session ends May 13, 2026. The law's final form and effective date remain uncertain. Institutions should monitor developments closely and consult counsel on current obligations.

What: Even under legal uncertainty, the law's core framework remains instructive. As written, it imposes a general duty of "reasonable care" on both developers and deployers of high-risk AI systems to protect consumers from algorithmic discrimination. Core requirements include:

- Public-facing disclosures when high-risk AI systems influence significant decisions
- Specific adverse action notifications to consumers explaining the AI's role and consumer rights
- Annual impact assessments evaluating discrimination, bias, and consumer risk
- Proactive monitoring, periodic testing, and bias mitigation

NIST/CRI ALIGNMENT — THE COLORADO SAFE HARBOR:[4,25,26]

Colorado provides the most explicit NIST connection of any state law. Deployers must implement a risk management program aligned with NIST AI RMF, ISO/IEC 42001, or another recognized framework designated by the Attorney General (AG). Compliance creates a rebuttable presumption of reasonable care and an affirmative defense, provided the entity also took proactive steps (adversarial testing, internal reviews, feedback processes) to discover and correct violations. Banks, credit unions, and affiliates subject to examination by a state or federal prudential regulator under published AI guidance may be deemed in full compliance if that guidance meets the Act's criteria.

Practical implication: adopting the CRI FS AI RMF positions your institution for the Colorado safe harbor while simultaneously generating compliance evidence for other jurisdictions. This holds true regardless of how SB-189 resolves: the underlying governance work is not wasted effort.

Implication: The enforcement pause does not eliminate AI governance risk. Institutions using AI in high-risk contexts should continue building proactive compliance programs. If the law takes effect in its current or amended form, institutions with documented NIST/CRI-aligned programs will be best positioned. Non-compliance risks under the existing statute include state AG enforcement (violations treated as deceptive trade practices, fines up to $20,000 per violation) and reputational damage.[25]

Action Items:

1. Monitor SB-189 and federal litigation developments through May 2026 and beyond.
2. Inventory all high-risk AI systems currently deployed or planned.
3. Implement or update a risk management program aligned with the NIST AI RMF or CRI FS AI RMF to establish the safe harbor defense.
4. Draft or update public disclosures and adverse action notices.
5. Establish a repeatable process for annual AI impact assessments covering bias, discrimination, and fairness.
6. Do not stand down on compliance preparation. The governance infrastructure built now serves your institution across multiple jurisdictions regardless of Colorado's final outcome.

3c. New York: The RAISE Act

Context: New York's RAISE Act was signed December 19, 2025, taking effect January 1, 2027. It was signed just eight days after the White House Executive Order seeking to preempt state AI regulation.[5,6,19]

What: The RAISE Act targets large frontier AI model developers, specifically those spending $100M+ on compute or meeting the $500M revenue threshold under chapter amendments. Covered developers must:[6,22]

- Create, publish, and comply with detailed safety and security protocols[5]
- Report incidents to the State within 72 hours[5]
- Submit to annual protocol reviews[5]
- Provide whistleblower protections for employees[27]

NIST/CRI ALIGNMENT — INDIRECT BUT SIGNIFICANT:[21]

The RAISE Act does not directly reference NIST or CRI as safe harbors. However, it allows NY regulators to deem certain federal standards equivalent to state transparency requirements.

The oversight office is housed within DFS, the same agency enforcing NY's aggressive Part 500 Cybersecurity Regulation. Enforcement will carry financial-regulator intensity.

Implication: While primarily targeting large base-model LLM developers, financial institutions using frontier AI models from covered developers should expect downstream implications for vendor due diligence, contract terms, and incident response. The Act applies to models "developed, deployed, or operating in whole or in part in New York State."[5,22,28]

Action Items:

1. Determine whether any AI models your institution uses meet the RAISE Act's "frontier model" definition.
2. Update vendor contracts to address incident notification requirements and safety protocol references.[22]
3. Monitor for NYDFS rulemaking and guidance from the new oversight office.
4. Coordinate compliance programs using the CRI FS AI RMF as a risk management baseline.

3d. California: A Layered AI Regulatory Landscape

Context: California's approach involves three distinct but overlapping pieces of legislation.

CCPA/CPRA Updates: The Baseline

What: Requirements include pre-use notice before using personal data in AI/ADM systems, the right to opt-out of solely automated decisions, and access and appeal rights for consumers to understand and challenge automated decisions.

SB-53: Profiling and Bias Accountability

What: SB-53 applies to "automated decision tools" for consequential decisions. It requires annual impact assessments, enhanced consumer notice, detailed reporting to the Civil Rights Department, and evidence of bias mitigation measures. It is more prescriptive than CCPA about bias assessment and regulator reporting.

AB 2013: Generative AI Transparency

What: AB 2013 requires disclosure of training data, methodology, and risks for generative AI models. It is uniquely focused on the provenance and mechanics of AI itself, going deeper than anything in NIST or CRI.

California Laws: Quick Comparison

Law	Focus	Unique Provisions	Consumer Rights
CCPA/CPRA Updates	All businesses using AI/ADM with CA consumer data	Pre-use notice, opt-out, access, appeal	Broadest: notice, opt-out, access, contest
SB-53	High-impact profiling by automated decision tools	Annual bias audits, regulator reporting	Notice + evidence of bias mitigation
AB 2013	Generative AI and ADM transparency	Training data, methodology, risk disclosure	Detailed transparency on how AI is built/trained

NIST/CRI ALIGNMENT — PARTIAL COVERAGE: California's laws do not reference NIST or CRI as safe harbors. Adopting CRI supports compliance but AB 2013's training data transparency requirements go beyond any federal framework. Many institutions will need to comply with all three laws simultaneously.

Action Items:

1. Inventory AI tools used with California consumer data across lending, fraud detection, customer service, and marketing.
2. Layer compliance: CCPA baseline, then SB-53 bias audits, then AB 2013 transparency disclosures.
3. For generative AI systems, prepare to disclose training data, methodology, and risk factors beyond NIST/CRI.
4. Assess whether impact assessments under Colorado or EU AI Act can be adapted for SB-53.

3e. Michigan: DIFS Bulletin 2026-03

Context: On January 14, 2026, Michigan DIFS issued Bulletin 2026-03. This is not a new law but an enforcement signal with immediate governance expectations. It applies to all state-regulated financial service providers.[7,8]

What: Institutions must maintain a written AI Systems Program (AIS Program) addressing:[7,8]

- Governance: transparent policies, accountability, multidisciplinary oversight for all AI lifecycle stages[9]
- Risk management controls: data quality, model accuracy, bias detection, vendor oversight[7]
- Internal audit functions[7]
- The ability to explain AI-driven outcomes to consumers and regulators[29]

Even institutions not formally using AI must establish an employee AI acceptable use policy.[9]

NIST/CRI ALIGNMENT — REFERENCED BUT NOT A SAFE HARBOR: [9]

Michigan's bulletin explicitly references the NIST AI RMF as an appropriate framework for AIS Programs. However, it does not provide a formal safe harbor or affirmative defense. The bulletin also references the U.S. Treasury's 2024 AI report as guidance.

Practical implication: "AI made the decision" is not a defense for adverse consumer outcomes.

Implication: Because this is a bulletin, expectations apply now. The scope covers any "analytical and computational technologies" used to make or support consumer-impacting decisions, not just systems explicitly labeled as "AI."[7,8]

Action Items:

1. Establish a written AIS Program documenting all AI system uses, governance controls, and risk management procedures.
2. Ensure your AIS Program is proportionate to consumer risk. DIFS expects a risk-based approach.[7]
3. Test, monitor, and update AI models for fairness, accuracy, and consumer impact on an ongoing basis.
4. Prepare executives and compliance teams to respond to DIFS examination inquiries with documentation.
5. Even if not using AI, establish an employee AI acceptable use policy.[9]

---

4. Putting It All Together: Compliance Overlap Map

The table below maps key compliance requirements across jurisdictions, showing where CRI FS AI RMF provides coverage and where additional work is needed.

Requirement	NIST/CRI?	Colorado	New York	California	Michigan	SEC
Written AI governance	Yes	Required	Required (devs)	Required	Required (AIS)	Expected
Risk/impact assessments	Yes	Annual + post-mod	Annual review	Annual (SB-53)	Proportionate	Expected
Bias testing & fair lending	Yes (CRI)	Reasonable care	N/A (dev-focused)	Annual audits	Required	Expected
Consumer disclosure	Partially	Pre-decision + adverse	N/A	Pre-use + opt-out	Required	Accurate disc.
Incident reporting	Yes (CRI)	90-day to AG	72-hour	Per CCPA	Per existing law	Per Reg S-P
Training data transparency	No	Not required	Not required	Required (AB 2013)	Not required	Not required
Third-party oversight	Yes (CRI)	Impact scope	Vendor protocols	Impact scope	Required	Required
NIST safe harbor	N/A	Yes (affirm. defense)	No (equiv. possible)	No	No (ref. only)	No
Exam-ready evidence	Yes (CRI)	Supports	Supports	Supports	Supports	Supports

THE BOTTOM LINE: Adopting the CRI FS AI RMF gives multi-state institutions the strongest single foundation across all current jurisdictions. Where it falls short, supplement with jurisdiction-specific measures: California's AB 2013 for training data transparency, New York's RAISE Act for vendor due diligence on frontier models, and Colorado's specific adverse action notice requirements. The federal preemption question remains unresolved. Until it is, comply with the most stringent applicable standard.

---

5. We Want to Hear from You

What topics should we cover next? Are there specific regulatory developments, enforcement actions, or emerging technologies you're watching? Let us know what is keeping you up at night.
How can we help? Verapath's team is here to support you! From gap analyses and framework mapping to automated control monitoring and examination preparation.

Reach out to us at aleccrawford@verapath.com or reply directly to this newsletter. We read every response.

---

6. Sources & Citations

[1] Cyber Risk Institute, "Financial Services Industry Unites to Launch Comprehensive AI Risk Management Framework," February 12, 2026. https://cyberriskinstitute.org/financial-services-industry-unites-to-launch-comprehensive-ai-risk-management-framework/

[2] U.S. Department of the Treasury, "Treasury Releases Two New Resources to Guide AI Use in the Financial Sector," Press Release sb0401, February 19, 2026. https://home.treasury.gov/news/press-releases/sb0401

[3] Colorado General Assembly, SB 25B-004, "Increase Transparency for Algorithmic Systems" (delaying SB 24-205 effective date to June 30, 2026), signed August 28, 2025. https://leg.colorado.gov/bills/sb25b-004

[4] Colorado General Assembly, SB 24-205, "Consumer Protections for Artificial Intelligence," signed May 17, 2024, effective June 30, 2026. https://leg.colorado.gov/bills/sb24-205

[5] Office of Governor Kathy Hochul, "Governor Hochul Signs Nation-Leading Legislation to Require AI Frameworks for AI Frontier Models," December 22, 2025. https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-require-ai-frameworks-ai-frontier-models

[6] Jones Walker LLP, "New York's RAISE Act: What Frontier Model Developers Need to Know," January 2, 2026. https://www.joneswalker.com/en/insights/blogs/ai-law-blog/new-yorks-raise-act-what-frontier-model-developers-need-to-know.html

[7] Michigan Department of Insurance and Financial Services, Bulletin 2026-03-BT/CF/CU, "Use of Artificial Intelligence Systems By Financial Service Providers," January 14, 2026. https://www.michigan.gov/difs/-/media/Project/Websites/difs/Bulletins/2026/Bulletin_2026-03-BT-CF-CU.pdf

[8] Michigan DIFS Press Release, "DIFS Issues Bulletin to Address Use of Artificial Intelligence in the Financial Services Industry," January 14, 2026. https://www.michigan.gov/difs/news-and-outreach/press-releases/2026/01/14/difs-issues-bulletin-to-address-use-of-artificial-intelligence-in-the-financial-services-industry

[9] Foster Swift Collins & Smith, "New DIFS Bulletin Regarding Use of AI by Financial Service Providers," JD Supra, March 23, 2026. https://www.jdsupra.com/legalnews/new-difs-bulletin-regard-use-of-ai-by-3778143/

[10] U.S. Securities and Exchange Commission, Division of Examinations, "2026 Examination Priorities," Fiscal Year 2026. https://www.sec.gov/examinations

[11] KPMG, "Deconstructing the Cyber Risk Institute Financial Services Artificial Intelligence Risk Management Framework," March 2026. https://kpmg.com/us/en/articles/2026/deconstructing-cyber-risk-institute-fs-ai-rmf.html

[12] National Institute of Standards and Technology, "AI Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, January 26, 2023. https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence

[13] Valdez Ladd, "A New Framework for AI Financial Services Audits," Medium, March 2026. https://medium.com/@oracle_43885/a-new-framework-for-ai-financial-services-audits-911cdea4f6c2

[14] Lowenstein Sandler LLP, "Financial Services AI Risk Management Framework: Operationalizing the 230 Control Objectives Before the Market Wakes Up," March 12, 2026. https://www.lowenstein.com/news-insights/publications/client-alerts/financial-services-ai-risk-management-framework-operationalizing-the-230-control-objectives-before-the-market-wakes-up-data-privacy

[15] Swept AI, "The CRI FS AI RMF: What 108 Financial Institutions Agree AI Risk Management Actually Requires," March 2026. https://www.swept.ai/post/cri-fs-ai-rmf-financial-services-ai-risk-management-framework

[16] Cyber Risk Institute, "Financial Services AI Risk Management Framework," framework and companion materials. https://cyberriskinstitute.org/artificial-intelligence-risk-management/

[17] Kroll, SEC Compliance Guide on Regulation S-P Amendments (adopted 2024, phased compliance December 3, 2025 for large firms, June 3, 2026 for others).

[18] White House, Executive Order, "Ensuring a National Policy Framework for Artificial Intelligence," December 11, 2025.

[19] Davis Wright Tremaine, "New York Enacts RAISE Act for AI Transparency Amid Federal Preemption Debate," December 2025. https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2025/12/new-york-raise-act-ai-safety-rules-developers

[20] White House, "National Policy Framework for Artificial Intelligence: Legislative Recommendations," March 2026.

[21] Mintz Levin, "NY Enacts RAISE Act Amid Federal AI Security Push — AI: The Washington Report," February 6, 2026. https://www.mintz.com/insights-center/viewpoints/54731/2026-02-06-ny-enacts-raise-act-amid-federal-ai-security-push-ai

[22] Jones Walker LLP, "New York's RAISE Act: What Frontier Model Developers Need to Know," January 2, 2026. https://www.joneswalker.com/en/insights/blogs/ai-law-blog/new-yorks-raise-act-what-frontier-model-developers-need-to-know.html

[23] Akin Gump, "Colorado Postpones Implementation of Colorado AI Act, SB 24-205," September 22, 2025. https://www.akingump.com/en/insights/ai-law-and-regulation-tracker/colorado-postpones-implementation-of-colorado-ai-act-sb-24-205

[24] Davis Wright Tremaine, "Mile-High Risk: Colorado Enacts Risk-Based AI Regulation to Address Algorithmic Discrimination," May 2024. https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2024/05/colorado-enacts-first-risk-based-ai-regulation-law

[25] Foster Graham Milstein & Calisher, "Colorado's Artificial Intelligence Act: What Businesses Need to Know About SB 24-205," December 17, 2025. https://fostergraham.com/2025/12/colorados-artificial-intelligence-act-what-businesses-need-to-know-about-sb-24-205/

[26] STACK Cybersecurity, "Colorado AI Act (SB 24-205) Compliance Guide," January 30, 2026. https://stackcyber.com/posts/ai-colorado-laws

[27] Nelson Mullins, "New York Laws 'RAISE' the Bar in Addressing AI Safety: The RAISE Act and AI Companion Models," January 12, 2026. https://www.nelsonmullins.com/insights/alerts/privacy_and_data_security_alert/all/new-york-laws-raise-the-bar-in-addressing-ai-safety-the-raise-act-and-ai-companion-models

[28] New York State Assembly, Bill A6453A / S6953B (RAISE Act), 2025–2026 Regular Sessions. https://www.nysenate.gov/legislation/bills/2025/A6453/amendment/A

[29] Insurance Journal, "Michigan Bulletin Provides Guidance for AI Use in Financial Services," January 20, 2026. https://www.insurancejournal.com/news/midwest/2026/01/20/854912.htm

Disclaimer

This newsletter is published by Verapath for general informational and educational purposes only. It does not constitute legal, regulatory, compliance, financial, or professional advice, and should not be relied upon as such. Receipt of this newsletter does not create an attorney-client, consultant-client, or other professional relationship between Verapath and any reader.

The regulatory landscape surrounding artificial intelligence is evolving rapidly. Laws, regulations, guidance, executive orders, and frameworks referenced herein are subject to change, amendment, delay, legal challenge, preemption, or repeal at any time, and may have changed since the date of publication. Effective dates and substantive requirements reflect our understanding as of the publication date. Readers should verify the current status of any statute, regulation, or guidance before taking or refraining from any action.

The content represents our interpretation and summary of publicly available information. Cross-jurisdictional analysis and framework alignment assessments are provided to aid general understanding and do not address the specific circumstances, operational footprint, or risk profile of any particular organization. References to third-party frameworks, agencies, and firms are for identification purposes only and do not constitute endorsement. Hyperlinks to external sources are provided as a convenience; Verapath is not responsible for the content of external websites.

Before taking or refraining from any action based on this newsletter, readers are strongly encouraged to consult qualified legal counsel and other appropriate experts who can evaluate the specific facts applicable to their institution. Verapath disclaims any liability for actions taken or not taken based on the contents herein.