STATE OF CONNECTICUT
Department of Banking
280 Trumbull Street | 16th Floor | Hartford, CT 06103

REGULATORY GUIDANCE: GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS

TO: **All Connecticut-chartered Financial Institutions and Other Entities Licensed or Regulated by the Connecticut Department of Banking**

FROM: **Jorge Perez, Banking Commissioner**

DATE: **September 22, 2026**

RE: **Governance of Artificial Intelligence Systems**

The Connecticut Department of Banking ("Department") is issuing this regulatory guidance to communicate its expectations regarding governance of AI Systems[1] used by Connecticut-chartered financial institutions and other entities licensed or regulated by the Department ("Regulated Entities"). This guidance applies to AI Systems used in both consumer-facing and internal functions, including without limitation, compliance, risk management, underwriting, pricing, fraud prevention, marketing, and customer service.

Use of Artificial Intelligence[2] ("AI") systems in the financial services industry may enhance efficiency, customer service, compliance, and risk management. AI Systems may also introduce operational, safety and soundness, cybersecurity, privacy, consumer protection, and other compliance risks.

I. AI Governance Framework

To manage the risks involved with use of AI Systems, the Department expects each Regulated Entity to develop and implement an effective governance framework ("AI Governance Framework") consistent with this guidance. The AI Governance Framework should:

[1] For purposes of this guidance, "AI System" means an automated system or tool that uses AI and materially influences business operations, risk management, or consumer-facing decisions of a Regulated Entity. Tools that use AI only incidentally, or whose output does not materially affect such operations or decisions, are outside the scope of this guidance. An AI System includes AI functionality embedded within a broader software product or service, including third-party or software-as-a-service tools, where that functionality meets the materiality threshold described above.

[2] For purposes of this guidance, "Artificial Intelligence" refers to any machine-based system trained on data that, for explicit or implicit objectives, generates outputs, including predictions, recommendations, decisions, or content, by using computational techniques that enable inference from data, and that operates with varying levels of autonomy. Artificial Intelligence does not include conventional analytical tools such as traditional rule-based engines, spreadsheet logic, or static calculations that do not involve inference from data. For example, a model that infers credit risk from historical data is Artificial Intelligence; a spreadsheet that applies fixed debt-income thresholds is not.

- Be appropriate to the size and activities of the Regulated Entity and proportionate to the scope, complexity, risk, and data sensitivity of the AI Systems used;
- Establish clear internal roles and oversight of AI Systems;
- Identify and manage potential risks of the AI Systems use, including cybersecurity, privacy, and protection of information systems and the consumer data and non-public information contained on those information systems, and integrate with the entity's overall risk management program;
- Incorporate best practices and recognized standards for AI Systems, cybersecurity, and privacy; and
- Ensure compliance with all applicable laws and regulatory requirements, including without limitation those relating to data security, privacy, record keeping and consumer protection.

The AI Governance Framework should include the following components:

A. Board & Senior Management Responsibility

Responsibility for the development, implementation, monitoring of AI Systems and the AI Governance Framework should be vested with senior management accountable to the board of directors, managing member, or other governing body of the Regulated Entity. The board of directors, managing members, or other governing bodies should take an active role in overseeing the entity's AI Systems and AI Governance Framework. This includes sufficient understanding of AI-related matters to exercise oversight, which may include the use of advisors; regular review of senior management reports on the AI Systems and Governance Framework; and confirmation that senior management has allocated sufficient resources to implement, maintain, and monitor them. The oversight and resources allocated should be proportionate to the scope, complexity, risk, and data sensitivity of the AI Systems involved.

B. Cybersecurity, Privacy, & Protection of Consumer Data

Ensuring cybersecurity, privacy, and protection of consumer information should be paramount in the development, implementation, monitoring, and oversight of the AI Systems and AI Governance Framework. Increased reliance on AI Systems, which often require the collection and processing of substantial amounts of data, may result in increased cybersecurity risks. Cyber-attacks on AI Systems could potentially expose sensitive non-public information, including consumer data. Such exposures could result in liability under applicable data security and privacy laws.[3] Therefore, assessing and mitigating these cybersecurity and privacy risks should be a primary focus of the AI Governance Framework. Regulated Entities should address these risks within their existing information security programs rather than through a separate or parallel cybersecurity regime. The controls applied should be risk-based and proportionate to the scope, complexity, risk, and data sensitivity of the AI Systems involved.

C. Incorporation of Best Practices and Standards

When developing and implementing an effective AI Governance Framework, Regulated Entities should review industry best practices and standards and incorporate those appropriate based on the entity's size, activities, and use of AI Systems. These may include, without limitation, governance frameworks and AI risk management standards developed by official standards organizations such as the National Institute of

[3] See e.g., Conn. Gen. Stat. § 36a-44a and Conn. Gen. Stat. § 36a-701b.

Standards and Technology (NIST) Artificial Intelligence Risk Management Framework, Version 1.0 and companion documents related to generative AI.[4] Regulated Entities are also encouraged to consider relevant supervisory guidance and risk management resources issued by federal financial regulators, including the National Credit Union Administration's materials addressing the use of AI and the U.S. Department of the Treasury's collaborative AI frameworks with the Financial Services Sector Coordinating Council (FSSCC).[5] Regulated Entities may also consider current federal model risk management principles, including model validation practices, where relevant to their use of AI Systems.[6]

D. Written AI Governance Plan

As part of the documentation of its overall AI Governance Framework, Regulated Entities should create a Written AI Governance Plan appropriate to the size and activities of the Regulated Entity and proportionate to the scope, complexity, and data sensitivity of the AI Systems used. The Written AI Governance Plan may be part of an entity's overall risk management plan.

D.1 Scope and Governing Principles of the Written AI Governance Plan

The Written AI Governance Plan should operationalize the three components of the AI Governance Framework described above, including:

- Board and senior management responsibility and oversight of AI Systems;
- Cybersecurity, privacy, and protection of information systems and the consumer data and non-public information contained on those information systems; and
- Incorporation of appropriate industry best practices and recognized standards for AI Systems, cybersecurity, and privacy.

These components apply across all elements of the Written AI Governance Plan. Accordingly, the plan should apply to internally developed AI Systems and address risk management of AI Systems provided or supported by vendors in alignment with the Regulated Entity's third-party risk management program and should support supervisory review and examination readiness.

---

[4] Nat'l Inst. of Standards and Tech., *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, (January 2023), https://doi.org/10.6028/NIST.AI.100-1; Nat'l Institute of Standards and Tech., *AI Risk Management Framework,* NIST AI RMF Playbook (January 26, 2023), https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-playbook. ***Other resources include***: U.S. Cybersecurity and Infrastructure Sec. Agency, Australian Signals Directorate's Australian Cyber Sec. Centre et al., *Principles for the Secure Integration of Artificial Intelligence in Operational Technology* (December 03, 2025), Principles for the Secure Integration of Artificial Intelligence in Operational Technology; N.Y. Dep't of Fin. Servs., *Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks*, (October 16, 2024), https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks; Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *ISO/IEC 42001:2023 Artificial Intelligence Management System* (2023), ISO/IEC 42001:2023(en), Information technology — Artificial intelligence — Management system.

[5] Nat'l Credit Union Admin., *Artificial Intelligence (AI)*, https://ncua.gov/regulation-supervision/ai (artificial intelligence resources); Fin. Sector Artificial Intelligence Exec. Oversight Grp., *Financial Sector Artificial Intelligence Executive Oversight Group Deliverables*, Financial Services Sector Coordinating Council, https://fsscc.org/aieog-ai-deliverables-full/

[6] See e.g., Cyber Risk Inst., *Financial Services AI Risk Management Framework*, https://cyberriskinstitute.org/artificial-intelligence-risk-management/ (intended to operationalize the NIST AI RMP and provide a structured approach for financial institutions to evaluate and managed AI-related risks). See Revised Guidance on Model Risk Management (Apr. 17, 2026), issued jointly by the Federal Reserve (SR 26-2), the FDIC (FIL-15-2026), and the OCC (Bulletin 2026-13), superseding the 2011 interagency guidance. Generative and agentic AI are outside the scope of the revised guidance pending further agency consideration.

D.2 Required Components of the Written AI Governance Plan

The Written AI Governance Plan should include the following components:

1) **Lifecycle:** Policies and procedures addressing the full lifecycle of AI Systems, including development or acquisition, testing and validation, deployment, monitoring, material changes, and retirement or decommissioning. Lifecycle governance should be commensurate with the nature, risk, and impact of the AI System and include appropriate controls for pre-deployment testing, ongoing performance monitoring, detection of model drift or degradation, change management, and orderly deactivation or retirement when appropriate.

2) **Inventory, Risk assessment, and management of AI Systems, including cybersecurity risks and data governance**: Processes for inventorying AI Systems, and identifying, assessing, tiering, and managing risks associated with AI Systems, including operational, safety and soundness, cybersecurity, privacy, data sensitivity, data collection, data quality and consumer protection risks. Risk management practices should be risk-based and proportionate to the scope, complexity, risk, and potential impact of the AI System, integrated with the Regulated Entity's broader risk management framework, and include appropriate escalation and remediation processes. Risk management should support differentiation and tiering among AI Systems based on materiality, data sensitivity, and potential consumer impact.

3) **Policies and procedures to ensure AI Systems comply with applicable laws**: Governance mechanisms addressing applicable federal and state laws, regulations, and supervisory guidance, including those relating to consumer protection, privacy, data use, and unfair or discriminatory practices. These mechanisms should support identifying relevant legal obligations, monitoring compliance over time, and responding to changes in law, regulation, or supervisory guidance. They should include monitoring for potential unfair or discriminatory outcomes, consistent with existing federal and state fair lending laws such as the Equal Credit Opportunity Act and the Fair Housing Act and their implementing regulations and should rely on existing escalation, remediation, and human oversight controls to address elevated risk of consumer harm or legal noncompliance.

4) **Human oversight of AI Systems**: Defined human oversight of AI Systems, including clear responsibility for AI-supported decisions, escalation protocols, and accountability for outcomes affecting consumers or regulated activities. Human oversight should be appropriate to the nature and impact of the AI System and sufficient to detect, review, and address errors, unintended outcomes, or potential consumer harm, including the ability to intervene, override, or take corrective action when warranted.

5) **Training and competency**: Policies and procedures to ensure that board members, senior management, and relevant personnel receive training that is risk-based and proportionate to their roles and to the risk, complexity, and consumer impact of the AI Systems used. Such training should address, as applicable, AI System functionality, limitations, risks, data governance, consumer protection considerations, and applicable legal and regulatory requirements, and should be updated periodically to reflect material changes in AI Systems use, technology, or regulatory expectations.

6) **Third-party risk management**: Governance of AI Systems provided or supported by third-party vendors, including appropriate due diligence, contractual controls, audits, and ongoing monitoring throughout the relationship lifecycle. Third-party governance should be consistent with the Regulated Entities overall third-party risk management practices and reflect the risks posed by the AI System, the data involved, and the extent of reliance on the third party.

7) **Documentation**: Documentation appropriate to the size and activities of the Regulated Entity and proportionate to the scope, complexity, risk, and data sensitivity of the AI Systems, sufficient to support internal governance, supervisory review, and examination readiness. Documentation should be maintained at a level appropriate to the AI System's risk and complexity and support transparency, accountability, and effective oversight, including documentation of AI System purpose, data sources, risk assessments, testing and validation, monitoring, governance approvals, and material changes.

II. Supervisory Expectations

Regulated Entities are encouraged to engage proactively with the Department regarding emerging uses of AI Systems. The Department plans to review AI Systems, AI Governance Frameworks, Written AI Governance Plans, and related policies and procedures during supervisory examinations.

In addition, the Department expects that AI Systems be transparent and explainable in a manner appropriate to their risk and consumer impact. At a minimum, Regulated Entities should be able to explain in a clear and concise manner whether AI Systems materially affect consumers and decisions regarding consumers.