# GSE Guidance on AI

## The new rules of accountability

December 2025

**Government-Sponsored Enterprise's (GSEs)[1] new bulletin is a market-defining event that transforms AI governance from a theoretical policy exercise into an operational discipline requiring verifiable proof. It's no longer about *having* a framework; it's about *proving its effectiveness* at the individual AI systems and model levels every day. This creates distinct, tangible challenges and opportunities across the organization.**

### Part 1: The Executive Summary - GSE Guidance on AI

Recent guidance from the GSEs has formally shifted the use of artificial intelligence from an operational advantage to a C-suite-level risk, mandating new standards for accountability, validation, and liability.

The New Reality: The guidance from GSEs on AI governance, including a notable bulletin with a firm March 2026 deadline, has fundamentally changed the risk landscape for the mortgage ecosystem. What was once considered a best practice has now become a non-negotiable requirement for doing business.

The Core Mandate: While the guidance introduces several new governance requirements, one clause elevates all others in significance: the seller/servicer must indemnify the GSE against all liabilities, losses, and damages arising from the use of their AI systems.

The Bottom Line: This transfer of liability makes AI governance a core strategic and balance sheet concern. It is no longer a technical project confined to IT or data science teams; it is a C-suite issue with direct financial implications for every stakeholder involved, from originator to investor.

### Part 2: The Three Core Mandates – What "Good" Looks Like

| Theme | What's Required | The Business Impact |
|---|---|---|
| Formalized Accountability & Ownership | AI-related policies must be formally approved by Senior Management (e.g., CIO, CRO). A designated owner must be appointed for the AI governance framework, and the roles and responsibilities for managing AI risk must | Accountability is being pushed directly to the C-suite. Named individuals are now answerable to regulators and business partners, requiring a clear, functional operating model, not just names on an organizational chart. |

| | | |
|---|---|---|
| | be clearly documented and understood across the enterprise. | |
| Continuous Validation & Evidence | The GSE guidance demands a system for ongoing risk management and validation of AI models. This isn't a vague suggestion; it means having a structured framework for regular audits covering security, bias, and performance. | This marks the shift from "V1" governance (having a policy) to "V2" (proving it works, continuously). To meet this requirement, institutions need a robust, pre-built methodology. This is precisely why industry-vetted frameworks like the newly incoming CRI AI Risk Management Framework are so critical. They provide detailed control objectives and testing procedures needed to generate the continuous evidence the GSEs will demand. |
| Full Transparency & Liability | Seller/servicers must be prepared to disclose the types of AI/ML systems they use, how those systems function, and what safeguards are in place upon request. Critically, they assume all financial liability via the indemnification clause. | The financial risk of AI failure now sits entirely with the seller/servicer and, by extension, their partners. You must have a "single source of truth" (a comprehensive AI inventory) to respond to disclosure requests accurately and a governance framework robust enough to withstand legal and financial scrutiny. |

In short, the bulletin signals a major shift from implicit expectations to explicit liability. While many organizations already treat AI as a core business function, this guidance formalizes the rules, demanding demonstrable proof of robust oversight, continuous validation, and an acceptance of full financial liability.

## Part 3: The Ripple Effect – What This Means for Your Role

This mandate creates a ripple effect, impacting every participant in the mortgage ecosystem differently.

**For Seller/Servicers (Lenders, Servicers):**
Your challenge is Direct Compliance & Financial Risk. You are the focal point of the mandate. You must build and prove a compliant framework not only to satisfy regulators but to protect your own balance sheet from the new liability you now hold.

**For Capital Markets Firms (Investment Banks, Dealer Groups):**
Your challenge is Inherited Risk & Due Diligence. The value and security of the assets you buy, package, and trade now directly depend on the AI compliance of your originating partners. A new layer of AI-specific due diligence is required to avoid acquiring hidden liabilities.

**For Technology & Service Vendors:**
Your challenge is Supply Chain Risk & Competitive Opportunity. The seller/servicers you support will now demand contractual proof that your platform is compliant and will not expose them to risk. This is a new hurdle, but also a significant opportunity to become a certified, "AI Governance Ready" partner and a winner in the market.

## Part 4: The KPMG Path Forward – Assess, Remediate, Certify

KPMG LLP (KPMG) provides a clear, phased path to not only achieve compliance but to build a robust, trustworthy AI program that creates a competitive advantage. Our services are structured to meet you where you are.

1. ASSESS: Your Readiness Roadmap

- AI Governance Readiness Assessment: A fast, targeted engagement to benchmark your current state against the GSE guidance and deliver a prioritized action plan.
- Third-Party AI Due Diligence Framework: For capital markets firms, we help you design and build the new framework to evaluate the AI risk of your partners and investments.
- Validation & Testing Services: Independent, technical testing of your AI models for bias, security, fairness, safety and performance to generate the evidence required for validation.

2. REMEDIATE & BUILD: Closing the Gaps

- AI Governance Implementation: Hands-on support to develop clear policies, implement technical controls, and design effective, repeatable testing procedures.
- Centralized AI Inventory: Build and maintain a thorough, enterprise-wide inventory of all AI systems, creating a single source of truth for risk management, compliance, and strategic oversight.
- AI Vulnerability Management: Provide a dynamic and AI-specific framework embedded within your existing vulnerability management program to evaluate, prioritize and remediate AI vulnerabilities.

3. CERTIFY & OPERATE: Building Long-Term Trust

- AI Governance Managed Services: For organizations that want to focus on their core business, we can operate components of your ongoing AI monitoring, testing, and reporting as a managed service.

The March 2026 deadline is closer than it appears.

TAKE ACTION NOW: Contact us for a complimentary GSE AI Guidance Readiness Briefing to discuss how these changes will impact your specific business.

[1] Source: Freddie Mac Single Family; Use of artificial intelligence and machine learning; March 3, 2026.

## Contact us


**Matt Miller**
**Partner & KPMG US Banking Cybersecurity Leader**
E: matthewpmiller@KPMG.com

**Bryan McGowan**
**Partner & KPMG US Trusted AI Leader**
E: bmcgowan@kpmg.com

**Kelly Combs**
**Managing Director & KPMG US Trusted AI Leader**
E: kcombs@kpmg.com

**Katie Boswell**
**Managing Director & KPMG Securing AI Leader**
E: katieboswell@kpmg.com




**Learn about us:** **kpmg.com**