

Risk Management Guide

for

HousingAI

Assessing and Managing the Risks of AI-Powered Regulatory Guidance

Organisation	[Your Organisation Name]
Prepared by	[Name / Role]
Date	[Date]
Version	[1.0]

1. Introduction

This guide provides a structured framework for assessing and managing the risks associated with adopting HousingAI as your regulatory guidance platform. It focuses specifically on the risks of using AI in a compliance-critical environment and provides practical mitigations for each.

Adopting any new technology involves risk. Adopting an AI-powered tool in a regulatory context requires particular care, because the outputs inform decisions that affect compliance, resident safety, and organisational governance. This guide helps your organisation evaluate those risks honestly and plan for them effectively.

Guidance: *This document is part of the HousingAI adoption toolkit. It is complemented by the Business Case and Implementation Guide.*

2. AI-Specific Risks

Using AI for regulatory guidance introduces a distinct set of risks that differ from traditional software adoption. Understanding these is essential for responsible adoption.

2.1 Accuracy and Hallucination Risk

Large language models can generate plausible-sounding but incorrect information — known as “hallucination.” In a regulatory context, this could mean incorrectly interpreting a requirement, citing a superseded standard, or conflating guidance from different regulatory bodies.

How HousingAI Mitigates This

- **Retrieval-Augmented Generation (RAG):** HousingAI grounds its responses in a curated, authoritative knowledge base of regulatory documents, not open internet content
- **Source attribution:** Every piece of guidance references the specific regulatory document, section, and date, enabling verification
- **Continuous curation:** The regulatory corpus is maintained and updated by subject matter experts, not solely by automated ingestion
- **Confidence indicators:** Where guidance involves interpretation or judgement, this is flagged to the user

Your Organisation's Role

- Treat HousingAI as a knowledgeable assistant, not an infallible oracle — human judgement remains essential for high-stakes decisions
- Designate a compliance lead who periodically spot-checks outputs against primary regulatory sources
- Establish an escalation path for cases where AI guidance is unclear or seems inconsistent

2.2 Regulatory Currency and Completeness

Regulatory requirements change frequently. There is a risk that the AI knowledge base may not reflect the very latest changes, or may have gaps in coverage for niche or emerging areas.

How HousingAI Mitigates This

- Structured ingestion pipeline with defined SLAs for incorporating new regulatory publications
- Monitoring across all key regulatory bodies: RSH, Housing Ombudsman, Building Safety Regulator, DLUHC, and parliamentary activity
- Version tracking so users can see when the knowledge base was last updated for any given topic

Your Organisation's Role

- Maintain awareness that no system (human or AI) captures 100% of regulatory change instantaneously
- Continue existing horizon-scanning practices as a complement during the initial adoption period
- Report any identified gaps or outdated content to HousingAI for rapid remediation

2.3 Over-Reliance and Deskilling

A significant risk with any AI tool is that staff may become overly dependent, leading to gradual erosion of in-house regulatory knowledge. If the tool became unavailable, the organisation could find itself less capable than before.

How HousingAI Mitigates This

- Role-based responses encourage understanding, not just compliance — explaining the “why” behind requirements, not just the “what”
- Source referencing encourages users to engage with primary documents
- Designed to augment human expertise, not replace it — handling volume and velocity so your team can focus on interpretation and strategy

Your Organisation's Role

- Frame HousingAI internally as a productivity and assurance tool, not a replacement for professional judgement
- Continue investing in staff CPD and regulatory training alongside AI adoption
- Periodically test organisational capability without the tool (e.g., through tabletop exercises)

2.4 Data Privacy and Information Security

Any cloud-based platform raises questions about data handling, especially in a sector that manages sensitive resident information.

How HousingAI Mitigates This

- HousingAI does not require access to resident personal data — it operates on regulatory content, not tenant records
- UK-hosted infrastructure compliant with public sector data handling standards
- Data processing agreement provided, aligned with UK GDPR requirements
- Cyber Essentials certification (or equivalent — details available on request)

Your Organisation's Role

- Conduct your standard supplier due diligence and information security assessment
- Include the platform in your information asset register and DPIA where required
- Review the data processing agreement with your DPO before implementation

2.5 Ethical AI Considerations

Housing providers operate in a context where fairness, transparency, and accountability are paramount. The use of AI should be consistent with these values.

- **Transparency:** HousingAI's guidance is explainable — it shows its reasoning and sources, rather than presenting opaque answers
- **Fairness:** Consistent regulatory guidance regardless of which team or individual is asking, reducing interpretation inconsistency
- **Accountability:** The audit trail enables retrospective review, demonstrating what the organisation knew and when
- **Human oversight:** All significant compliance decisions remain with qualified humans; the AI informs but does not decide

3. Example Risk Register

Guidance: Review each risk and adjust the ratings based on your organisation's specific context, risk appetite, and existing capabilities. Assign owners before commencing implementation.

Risk	Impact	Likelihood	Mitigation	Residual	Owner
AI provides inaccurate guidance	High	Low	RAG architecture, source attribution, human oversight, spot-checking	Low	[Compliance Lead]
Knowledge base not current	High	Low	Defined update SLAs, version tracking, complementary horizon scanning	Low	[Compliance Lead]
Staff over-reliance / deskilling	Medium	Medium	Position as augmentation tool,	Low	[Head of People]

			continued CPD, capability testing		
Data breach or security incident	High	Low	UK hosting, no PII required, DPA in place, Cyber Essentials	Low	[IT / InfoSec Lead]
Low user adoption	Medium	Medium	Phased rollout, executive sponsorship, role-specific demonstration, champions	Low	[Project Sponsor]
Vendor lock-in / discontinuity	Medium	Low	Standard data export, knowledge retained in-house, contractual exit provisions	Low	[Procurement Lead]
Staff or board resistance to AI	Medium	Medium	Clear communication about AI role, transparency, board briefing on responsible AI	Low	[CEO / Sponsor]
Regulatory body concerns about AI	Medium	Low	Transparency about AI as aid not replacement, audit trail shows human decision-making	Low	[Dir. of Governance]
Integration with existing systems	Low	Low	SaaS platform, minimal integration, API for future needs	Low	[IT Lead]
Cost overruns or unclear pricing	Medium	Low	Fixed subscription pricing, clear terms, ROI monitoring	Low	[Finance Lead]

--- End of Document ---