

AI Risk Management Tips — Top 3

1. Input Risks: Protect Confidential Data

Many AI platforms store user prompts and incorporate them into their training data, which means your input could resurface for someone else later. In short, assume there is no privacy or confidentiality for any prompts or data you provide to an AI tool.

Tip: Before entering any private, confidential, or personally identifiable information, understand the platform's security features. Jack Conway recommends limiting AI use to company-approved tools. Transactional information or data should never be uploaded outside of company-approved tools.

2. Output Risks: Review Before You Publish

Many AI platforms pull their data sets from the internet, which can include biased or discriminatory content. This means AI-generated text may create fair housing issues if used without review. AI can also produce inaccurate information, known as "hallucinations," or generate content that is uncomfortably similar to copyrighted material. Finally, AI-generated images and videos can mislead clients by depicting features that don't exist.

Tip: Review all AI-generated content for accuracy, fair housing compliance, and originality. Verify facts with independent sources. Modify AI output, particularly for written content, to make sure it is truly your own and to avoid intellectual property issues.

Label AI-generated or AI-enhanced images or videos clearly so viewers aren't misled. AI labeling requirements are being built into some state laws. Stay informed on AI policies and laws.

3. Fraud Risks: Protect Against AI-Driven Scams

Deepfake videos, voice impersonations, and spoofed emails are growing threats in real estate. These scams can compromise transactions and client trust. Share these safeguards with your clients and make them aware.

Tip: Independently verify email addresses, phone numbers, and text message senders, and warn your clients about these scams. Protect your passwords, email accounts, and transaction management platform access. When hosting video calls, send the invitations yourself and verify all participants. If you get a phone call, even if you recognize the voice on the other line, double check the number. And if the call involves financial details, verify that information independently before taking any action at all.