

AI Governance: Sample AI Use Request Processes

Vendor Management

The introduction of artificial intelligence (AI) into organizational systems and applications begins with vendor management and a software request form, with associated evaluation and approval workflows. This includes the addition of AI to existing software or new software.



Evaluations

The reviews focus on several key issues or concerns when evaluating whether the introduction of AI is within an acceptable risk level at the time.

QUESTIONS INCLUDE:

1. What model is the AI?
2. What data is the AI trained on?
3. Where is the data?
4. Where does the AI reside?
5. Are additional cybersecurity, compliance, and regulatory concerns addressed? Do the risks require a control plan to ensure regulatory compliance?

TWO PRIMARY CONCERNs:

1. (Negative) Employee impact (potential for bias, etc.)?
2. (Negative) Customer impact (potential for bias, etc.)?

If either answer is "yes" or has the potential for "yes," then a control plan is required to ensure the AI and associated processes are being used as intended and approved. Factors such as human-in-the-loop oversight, auditing, testing, and scheduled spot checking can be used to control for cybersecurity, compliance, and regulatory risks.

Tracking

AI systems evaluation documentation and applicable control plans are stored for tracking and audit purposes.