AI Governance Maturity Model: AI Chaos to Clarity

John W. Moran[1]

July 2026

Artificial intelligence (AI) is advancing rapidly, far faster than previous transformations. New models and AI applications are emerging at a rapid pace. This velocity of change poses unique security challenges as quick deployment often outpaces thorough risk assessment and control implementation. Consequently, security risks can become an afterthought. To manage these rapidly shifting risks and opportunities, public health leaders must stay actively informed.

To ensure responsible adoption of AI technology, it is important for organizations to develop and adopt a robust, unified governance policy. AI governance must be actively deployed, monitored, and updated—otherwise, it remains a static paper exercise.

Core focus areas of a unified governance policy are:

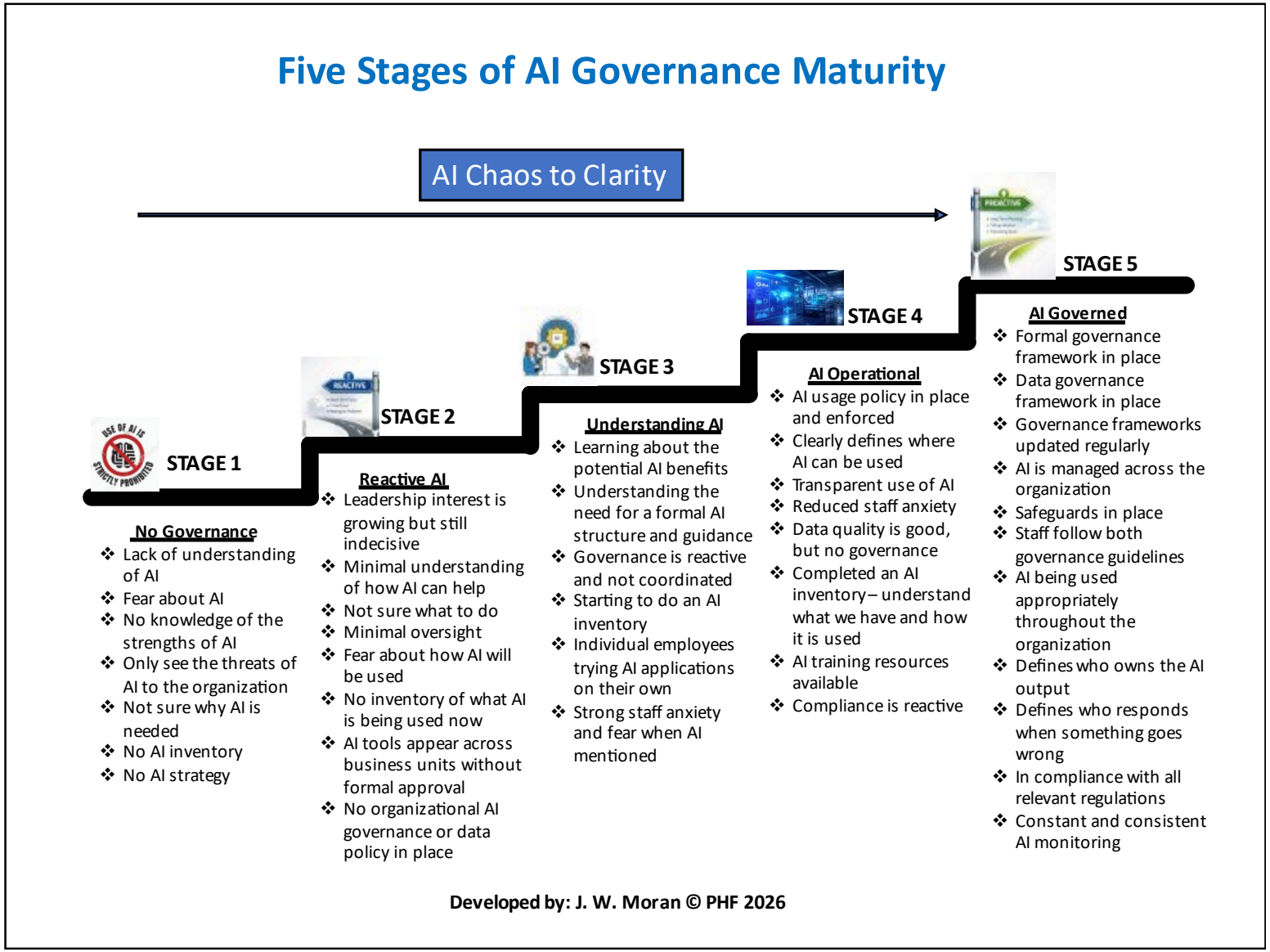
- *Visibility*: Track and visualize AI applications across the entire IT landscape.
- *Integration*: Safely embed AI capabilities into existing systems and processes.
- *Accountability*: Ensure AI models are used responsibly and for their intended purpose.
- *Data Stewardship*: Establish comprehensive data governance to augment the AI policy.
- *Lifecycle Management*: Oversee all active AI models, processes, and deployments.
- *Compliance*: Implement ethical and regulatory guardrails to meet legal standards.

Navigating the Five Stages of Maturity

To help agencies understand their current AI positioning, the Public Health Foundation (PHF) developed a Five Stages of AI Governance Maturity model as shown in Figure 1. This framework describes five distinct stages of operational

[1] Sr. AI and QI Advisor at PHF

readiness, each with specific operational characteristics. PHF provides targeted guidance, transition strategies, and curated resources to help health departments determine their starting point and advance systematically to the next level.



Implementation Strategy:

- *Keep it Simple*: Start with plain language instead of dense, multi-page documents.
- *Prioritize Utility*: A clear, one-page summary of "dos and don'ts" is more effective for daily compliance than a 70-page manual.
- *Scale Progressively*: Expand the complexity of the framework alongside your organizational growth.
- *Commit Continuously*: Treat AI and data governance as ongoing commitments that adapt quickly to new security threats and regulatory updates.

Conclusion:

Data governance and AI governance require a continuous organizational commitment that needs to grow and adjust to new compliance requirements as well as business and security challenges. Both need to be reviewed quarterly to stay relevant.