# The Phased AI Enablement Framework

*A Practical, Evidence-Based Maturity Model for Safe Enterprise AI Adoption*

**Christopher Kokoski**

AI Enablement | Learning & Development | Responsible Adoption

*A practitioner framework for helping people, not just tools, adopt AI well.*

## Executive Summary

Most organizations are adopting AI backwards. They deploy tools before building the human capability to use them, ship pilots before establishing guardrails, and treat training as an afterthought rather than the core of the work. The result is predictable: stalled adoption, runaway cost, compliance exposure, and a widening gap between the few who use AI well and the many who do not.

The evidence is stark. While 88% of organizations now use AI in at least one business function, only about 1% have reached genuine AI maturity, the point where AI is systematically embedded into workflows.

*Sources: McKinsey, 2025 (88% adoption); Iternal/USAII analysis, 2026 (~1% maturity).*

This framework offers a different approach, built on a simple principle drawn from real practice: AI enablement is a people problem, sequenced developmentally, with governance built in from day one. It lays out a phased path, 90 days, six months, one year, three years, and a five-year horizon, that starts people on small, safe, high-value tasks, measures what works, and scales deliberately. It is model-agnostic and tool-agnostic by design, because the durable capability is in how people and the organization adopt AI, not in any single vendor's product.

---

## Part 1: Why Most AI Adoption Fails

Before proposing a path forward, it is worth being honest about how AI adoption actually goes wrong in practice. The research points to four recurring failure modes.

### 1. Shadow AI: adoption happens with or without you

The single most important fact about enterprise AI is that employees are already using it, whether or not the organization has sanctioned it. This is shadow AI, and it is now the dominant operational reality.

*More than 80% of workers use unapproved AI tools (UpGuard, State of Shadow AI). Up to 65% of employees bypass IT to use unauthorized tools (industry analysis, 2026). Only 37% of organizations have any AI governance policy (IBM, 2025).*

Shadow AI is not driven by malice. It is driven by productivity pressure and inadequate approved alternatives: people choose speed, and when official tools lag behind what employees can access on their own, they route around them. The risk is real and quantified: shadow AI now accounts for roughly one in five data breaches, adding an average of $670,000 per incident, and most shadow AI tools fail standard compliance benchmarks.

*Sources: IBM 2025 Cost of a Data Breach Report; Normalyze, 2024 (76% of shadow AI tools fail SOC 2); Gartner, 2025 (40%+ of enterprises will face shadow-AI-linked incidents by 2030).*

**The lesson:** you cannot prevent AI adoption; you can only choose whether to guide it. A framework that ignores shadow AI is a liability disclaimer, not a strategy.

### 2. Policy without enforcement or alternatives

Many organizations respond to AI risk by writing a policy and considering the problem solved. The evidence shows this fails. Productivity pressure is the primary driver of shadow AI, which means a policy that bans tools without providing approved, capable alternatives simply pushes usage further underground. Policy without technical enforcement or a genuinely useful sanctioned option does not change behavior; it just removes visibility into it.

### 3. Tools dropped onto broken workflows

A common pattern: companies drop AI onto broken processes, ship models before thinking them through, and celebrate speed over results. Fast looks impressive, but adoption stalls, models gather dust, and return on investment stays invisible. AI applied to a broken workflow produces a faster broken workflow.

### 4. Training treated as an afterthought

This is the failure most directly relevant to enablement, and the most fixable. The data is clear that the bottleneck is human readiness, not technology.

> *82% of companies in early AI maturity have not yet implemented any talent strategy or training to prepare employees for AI-driven workflows (enterprise trends analysis, 2026). 57% of organizations cite skill gaps as the primary barrier to AI maturity (MIT CISR model). Organizations relying on self-directed learning see far lower adoption than those with structured programs.*

**The encouraging finding:** this is the variable an enablement program directly controls. Organizations with structured training programs see 3 to 4 times higher adoption than those relying on self-directed learning, and companies that allocate dedicated change-management resources see 2 to 3 times higher adoption than those that treat it as an afterthought.

> *Sources: AI Skills Gap analysis, 2026 (3-4x); Deloitte, State of AI in the Enterprise, 2024 (2-3x; recommends 20% of every AI initiative budget go to change management and training).*

---

## Part 2: The Principles Behind the Framework

The failures above point directly to the principles that should govern a better approach. Each principle is a direct response to documented evidence, and each reflects how effective AI enablement actually works in practice.

- **Adoption is a people problem, sequenced developmentally.** The tool is the easy part. Capability is built by moving people from small, safe wins to progressively more ambitious use, not by a one-time tool rollout.
- **Augment, do not replace.** The goal is people using AI to maximize their output and skill up, not people automating themselves away. This is both the ethical stance and the practical one: 87% of executives expect jobs to be augmented rather than replaced, and framing AI as augmentation is what wins the trust that drives adoption.
- **Governance from day one, not bolted on later.** In any regulated environment, and especially in healthcare under HIPAA, the guardrails come first. Responsible AI is not a compliance checkbox; 58% of executives say strong responsible-AI practices actually improve ROI and efficiency.
- **Provide the sanctioned alternative.** Because shadow AI is driven by inadequate options, the program must give people approved tools genuinely capable enough that they have no reason to route around them.
- **Measure, iterate, and turn what works into onboarding.** Every stage collects data. What proves out becomes standardized and embedded into how new people are brought on, so capability compounds rather than resetting with each hire.
- **Model-agnostic and tool-agnostic.** Vendors and models change constantly. The durable asset is the human and organizational capability to adopt AI safely, which transfers across whatever tools come next.

---

## Part 3: The Phased Framework

This is the core of the model: a developmental sequence that takes an organization from first safe steps to embedded capability. The timeline aligns with what the research shows is realistic, organization-wide AI capability typically requires three to six months of phased rollout just to reach broad basic proficiency, and full maturity unfolds over years, not quarters.

> *Timeline grounding: MIT CISR Enterprise AI Maturity Model (workforce education and pilots: 3-6 months; systematic integration: 12-24 months); AI Skills Gap analysis, 2026 (intermediate job-specific skills: 4-8 weeks; org-wide rollout: 3-6 months).*

### Phase 1, The First 90 Days: Safe, Small, High-Value Wins

The goal of the first quarter is not transformation; it is a successful beachhead. Start a broad group of people using AI for small, low-risk, high-frequency tasks where it clearly helps and where a mistake is cheap and reversible.

**Phase 1 starter tasks (low-stakes, high-frequency)**

Planning and outlining. Brainstorming and idea generation. Reviewing and giving feedback on work. Summarizing documents and threads. Light data interpretation. Getting help learning new tools and platforms. Studying and preparing for real certifications to skill up. These are the augmentation tasks that build confidence without touching sensitive data or high-stakes decisions.

Run a focused training on one or two of these tasks, have a group actually start using AI for them, and begin collecting data immediately: who is using it, for what, and whether it is helping. The guardrails, especially the rule that no protected or confidential information goes into an unapproved tool, are taught from the very first session. In parallel, stand up a small experimental group, people working on the bigger, harder friction points across different departments, ideally in sandbox or simulated environments where they can test and iterate safely.

- **Phase 1 success looks like:** a meaningful share of the pilot group using AI weekly for one or two safe tasks, an approved tool in place, baseline usage data flowing, and zero compliance incidents.

## Phase 2, Six Months: A Repertoire and Real Experiments

By the half-year mark, the goal is for the broad group to be comfortably performing three to five small tasks with AI, no longer a novelty but a normal part of how they work. The experimental group, meanwhile, has run several real tests on harder problems and produced early evidence about what works and what does not.

This is where measurement starts to pay off. The data from Phase 1 reveals which use cases stuck, which fell away, and where people got stuck, and that evidence guides what to teach next and which experiments to scale. Crucially, the things that prove out begin getting documented into repeatable practice.

- **Phase 2 success looks like:** broad competence on three to five tasks, a portfolio of completed experiments with honest results, refined training based on real usage data, and the first standardized playbooks emerging from what worked.

## Phase 3, One Year: From Practice to System

At the one-year mark, AI use is no longer a program running alongside the work; it is becoming part of the work. The proven use cases are integrated into standard workflows, the governance framework is established and understood, and, critically, an AI-enablement onboarding system exists so that every new hire is automatically trained to use AI within clear parameters from day one.

This is the point at which capability stops depending on the original champions and starts being institutional. The research describes this stage as systematic AI integration with governance frameworks and internal AI capability, typically reached over 12 to 24 months. An internal community, what many organizations call AI champions or a center of excellence, sustains momentum and spreads good practice across teams.

- **Phase 3 success looks like:** proven use cases embedded in standard workflows, a working onboarding system that skills up every new hire, an established governance framework, and a network of internal champions carrying it forward.

## Phase 4, Three Years: Embedded Capability and Selective Autonomy

Over a multi-year horizon, the organization moves from using AI for discrete tasks toward AI being embedded in how work is designed. The experimental track, having matured, can responsibly explore more advanced applications, including agentic and automated workflows, in the areas where they have been validated and where governance is strong enough to support them. Industry analysts expect a meaningful share of enterprise work to involve AI agents by the late 2020s; the organizations positioned to do this safely will be the ones that spent the prior years building the human capability and the guardrails first.

- **Phase 4 success looks like:** AI as a normal input to how work is designed, validated advanced and agentic use in well-governed areas, and a workforce that has skilled up alongside the technology rather than being displaced by it.

### The Five-Year Horizon: Durable, Adaptive Advantage

Five years out, the specific tools will have changed several times over, which is exactly why the framework is built on capability rather than any one product. The durable outcome is an organization that has institutionalized the ability to adopt whatever comes next: a workforce fluent in working alongside AI, a governance model that flexes as regulation and technology evolve, an onboarding system that keeps capability compounding, and a culture of measured, responsible experimentation. The five-year goal is not a particular technology; it is adaptive capability, the proven ability to absorb the next wave safely and turn it into advantage.

---

## Part 4: The Governance Thread

Governance is not a phase; it runs through every phase from the first day. Because shadow AI and compliance exposure are the most serious documented risks, the framework treats guardrails as the foundation rather than the finish line. The core commitments:

- No protected, confidential, or regulated information enters any AI tool that is not explicitly approved for it. In healthcare, manual de-identification is not assumed to satisfy HIPAA when using third-party systems without proper data agreements.
- AI output is a draft a human verifies, never final truth. A named person remains accountable for every result.
- Approved tools are provided that are capable enough to remove the incentive for shadow AI, paired with the visibility to know how AI is actually being used.
- Use is transparent, and the program is measured continuously so that guardrails can tighten or adapt as usage and regulation evolve.

Done well, governance is not the brake on adoption. Clarity about where the lines are is precisely what lets people use AI confidently rather than fearfully, which is why responsible-AI practice correlates with better, not slower, results.

---

## Closing: Enablement as a Discipline

The organizations that succeed with AI will not be the ones that bought the most tools or moved the fastest. They will be the ones that built the human capability to use AI well, sequenced the journey developmentally, and made safety the foundation rather than an afterthought. That is a discipline, and it is a learnable one.

This framework reflects how that discipline actually works in practice: start small and safe, prove value, measure relentlessly, scale what works, build it into onboarding, and keep people, not tools, at the center. The tools will keep changing. The capability to adopt them well is the durable advantage.

---



*Note on sources: statistics and findings throughout are drawn from publicly reported 2024 to 2026 research, including IBM, McKinsey, Deloitte, Gartner, MIT CISR, and industry analyses of enterprise AI adoption and governance. Figures are cited inline to credit those sources; this document synthesizes them into a practitioner framework.*