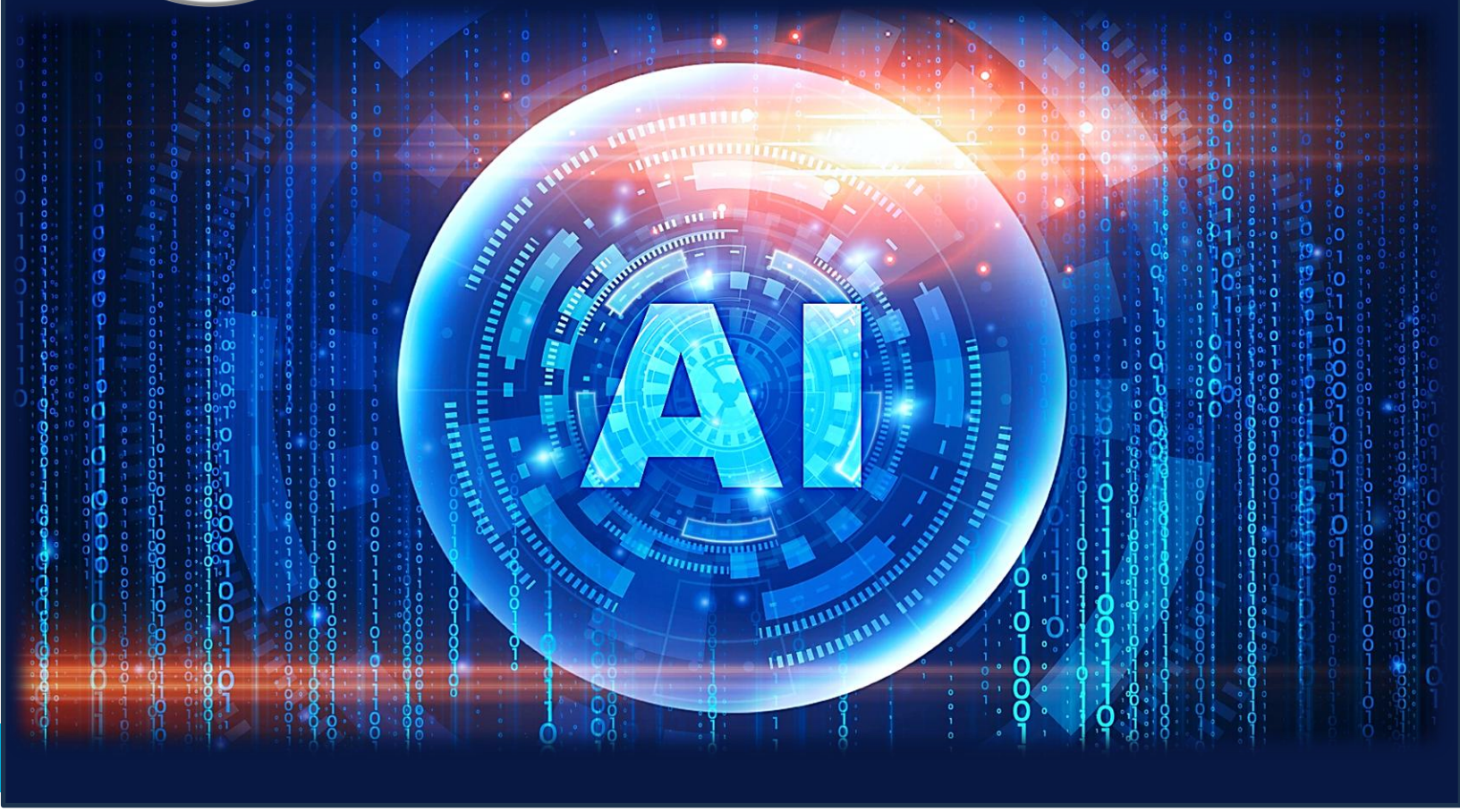
Smart Innovation Corporation Innovation Hub White Paper #3



AI Lifecycle Management

By:

Joseph Madden, President, Madden Consulting

Dr. Indu Singh, Managing Director & AI CTO, Smart Innovation Corporation

Smart Innovation Corporation

10640 Main St, Suite 300, Fairfax, VA 22030 USA

November 2025

SMART INNOVATION CORPORATION
INNOVATION HUB WHITE PAPER #3

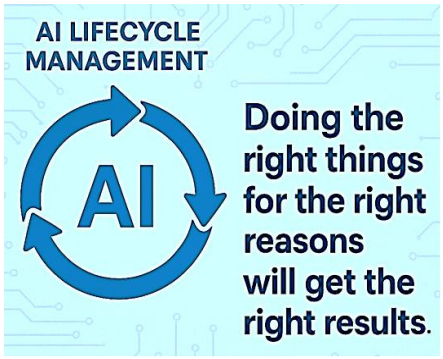
TABLE OF CONTENTS

1) ABSTRACT

The rise of artificial intelligence (AI) is reshaping industries, driving innovation, and creating new business opportunities. However, as with any complex software technology, building, deploying, and maintaining AI-enabled solutions requires a disciplined approach. **AI Lifecycle Management** encompasses the structured processes and best practices required to create cost-effective, high-quality, and secure AI-enabled solutions and manage them from inception to retirement. This white paper explores the phases of AI Lifecycle Management, core principles, and recommended best practices. It aims to guide organizations in implementing sustainable, scalable, and responsible AI systems.

2) INTRODUCTION

AI is the Third Technological Revolution which is now revolutionizing the world's societies with unparalleled speed and transformative impacts. AI's influence will further permeate every economic sector as well as all facets of our daily lives, ultimately paving the way for the emergence of the Fourth Technological Revolution: the Knowledge Society. As a result, it is imperative for organizations everywhere to immediately begin preparing to engage with and effectively use AI by following, at minimum, the proven approach to AI Lifecycle Management listed in this paper that covers many technical, organizational and ethical considerations.



AI Lifecycle Management refers to the seven stages that govern development and maintenance of AI-enabled solutions throughout the entire lifecycle. It addresses not only the functional and technical aspects of model development but also business alignment, integration with other systems, compliance, operationalization, and monitoring. With AI becoming central to strategic decisions, organizations must move beyond *ad hoc* development and adopt a lifecycle approach to ensure reliability, accountability, and business value.

AI development and peer reviews should leverage best practices in the NIST Secure Software Development Framework (SSDF), as well as the *NIST Special Publication 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models*.

3) GENERATIVE AI

Generative AI is model-based and can use inputs from text, images, audio and video recordings, and code, etc., to generate new content that has similar characteristics. For example, it can turn text inputs into an image or turn video recordings into text.

- Generative AI refers to a class of artificial intelligence models that have the ability to generate new content, such as images, text, or other types of data.
- These models are trained on large datasets and learn to generate content that is similar to the patterns present in the training data.

OpenAI's GPT models fall under the category of Generative AI. These models can generate coherent and contextually relevant human-like text based on the input they receive. Generative AI reaches across diverse sectors, encompassing natural language processing, visual computing, and artistic expression.

4) CORE PRINCIPLES OF EFFECTIVE AI LIFECYCLE MANAGEMENT

Core principles of effective AI Lifecycle Management should be organized in a way that covers the full spectrum from planning to post-deployment. There are five key considerations as shown below:

> ***KEY TAKEAWAY***
>
> ***"AI lifecycle management is important because it assists in sustaining the efficiency of the models in the future."***
>
> *Global Gurus*

A) GOVERNANCE & COMPLIANCE:

- Implement standards for ethics, fairness, and regulatory compliance.

B) COLLABORATION:

- Foster alignment between data science, engineering, and business teams.

C) AUTOMATION:

- Use MLOps tools to automate repetitive tasks and improve efficiency.

D) TRACEABILITY:

- Maintain detailed documentation of data, models, decisions, and changes.

E) SECURITY & PRIVACY:

- Safeguard sensitive data and models from unauthorized access.

5) AI LIFECYCLE MANAGEMENT: SEVEN KEY STAGES

There are seven distinct stages in AI Lifecycle Management as shown on the next page.

AI development and peer reviews should leverage best practices in the *NIST Secure Software Development Framework (SSDF), as well as the NIST Special Publication 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models.*

SEVEN KEY STAGES

STAGE	DESCRIPTION	CONTROL GATE(S)
1. PLANNING	Prepare business case, budget and schedule estimates and project plan for the AI-enabled solution.	Peer review
2. REQUIREMENTS	Develop functional & nonfunctional requirements (capabilities, features/use cases, user stories).	Peer review
3. DESIGN	Design the AI-enabled solution (architecture and data model, user interface model, business process flow, interface control document).	Peer review
4. DEVELOPMENT	Develop AI-enabled solution components. Gather, clean, and preprocess data. Train machine learning or deep learning models.	Peer review, Unit level testing
5. TESTING	Integrate components. Test model on validation data. Tune parameters and check metrics.	Integration test, System test
6. DEPLOYMENT	Prepare final release content and deploy into production.	Final release audit
7. MAINTENANCE	Track performance, detect drift, and gather user feedback. Retrain, fine-tune, or update models based on feedback. Retire outdated models and restart lifecycle with new initiatives.	Peer review, Unit level testing Regression test Maintenance release audit

5.1 PLANNING

Clearly defining the business problem ensures AI initiatives deliver measurable impact. This stage involves identifying key performance indicators (KPIs), aligning with organizational objectives, and engaging stakeholders. Once the business case is established, this stage also includes cost and schedule estimates and a project plan to include identification of risks and opportunities associated with the AI initiative. The quality control gate for this stage is a peer review and stakeholder approval of the business case, estimate and project plan.

5.2 REQUIREMENTS

Clearly identifying the functionality that will address the above business problem ensures that both the developer and customer have a common understanding of what the AI-enabled solution will do. For complex systems, requirements are typically decomposed down to three levels of abstraction:

A) **CAPABILITIES:** broad areas of functionality understandable by senior stakeholders

B) **USE CASES/FEATURES:** functionality that satisfies a specific user goal and is understandable to an end user

C) **USER STORY:** a testable thread of functionality that is a subset of a use case/feature and can be assigned to a developer

During this stage, it is important to identify the entire agreed-upon scope of the AI-enabled solution as well as what portion of that scope will be allocated to a minimum viable product. However, requirements details can be fleshed out in an iterative or agile fashion.

Requirements include both functional requirements and non-functional requirements (to include security requirements). The quality control gate for this stage is a peer review of requirements before any detailed design or development work begins for that requirement.

5.3 DESIGN

During the design stage, requirements are allocated solution components that comprise the design of the complete AI-enabled solution and which include both AI and non-AI components (e.g., custom code, COTS package(s), integrations with hardware devices, etc.). Typical artifacts from the design stage include: Solution Architecture and Data Model (to include a data governance approach), User Interface Model, Business Process Flow, and Interface Control Document.

Key design decisions should be based on an alternative analysis that uses risk adjusted objective criteria to weigh the best available options to meet customer functional and non-functional requirements to include security requirements. The quality control gate for this stage is a peer review of the overall solution architecture and data model before any detailed design or construction work begins and a peer review of the other design artifacts before any development work begins for that component.

5.4 DEVELOPMENT

This stage entails development of the AI-enabled solution's components which may include AI components as well as non-AI components such as Custom Code, COTS Package Implementation, Integrations with Hardware Devices, and Interfaces with Existing Systems.

The AI components depend on high-quality data. This includes data collection, cleaning, labeling, augmentation, storage, and compliance with regulations like GDPR. Data governance ensures

consistent standards and traceability. During development of AI components, data scientists experiment with algorithms, tune hyperparameters, and build models. Tracking experiments, code, and datasets is crucial for reproducibility. Collaboration tools facilitate communication between teams. The quality control gate for this stage is a peer review and unit test of each solution component before integration testing begins for that component. .

5.5 TESTING

This stage entails integration testing of each of the components that comprise the complete AI-enabled solution.

For the AI components, models must be rigorously evaluated using appropriate metrics (e.g., accuracy, precision, recall). Fairness and explainability are critical to avoid biased outcomes and ensure trust in AI systems. Once all components are integrated, an end-to-end system test is conducted that includes cybersecurity testing. The quality control gates for this stage include a peer review of test cases before formal testing begins and peer review of test summary results at the conclusion of formal testing prior to deployment.

5.6 DEPLOYMENT

This stage is where the AI-enabled solution is packaged and deployed into a production environment. Options include on-premise, cloud, or edge deployments. CI/CD pipelines can enable frequent and reliable model updates.

The quality control gate for this stage is a final release audit prior to deployment into the production environment. This should include a Software Bill of Materials (SBOM) which provides a detailed list of the components contained in the AI-enabled solution. To minimize cybersecurity risks, the final release audit should leverage best practices described in the NIST SSDF and *NIST Special Publication 800-218A*

5.7 MAINTENANCE & MONITORING

During the maintenance phase, customer feedback is collected to ensure the AI-enabled solution continues to meet stakeholder expectations. Bug fixes, enhancements and technology upgrades are performed as required.

For the AI components, continuous monitoring tracks model performance, data drift, and user feedback. When performance degrades, retraining or model replacement is necessary. Automated alerts and dashboards support proactive maintenance. The quality control gates for this stage are peer review, unit testing, regression testing and a maintenance release audit prior to deployment of a new version. When the AI-enabled solution becomes obsolete, it should be retired safely, preserving logs and documentation. In some cases, components can be reused or fine-tuned for new applications.

6) BEST PRACTICES FOR AI LIFECYCLE MANAGEMENT

AI Lifecycle Management must incorporate AI Best Practices. AI will continue to evolve for some time to come. The Best Practice approach ensures using AI in an effective manner, avoiding common pitfalls and AI management risks. Below is a summary discussion of recommended best practices for AI Lifecycle Management:

AI LIFECYCLE MGMT. AREAS	BEST PRACTICES	RECOMMENDATIONS
STRATEGY & PLANNING	• Align AI initiatives with clear business objectives and KPIs. • Start small with high-impact, low-risk use cases (proof of value). • Build cross-functional teams (data science, IT, legal, product, ethics).	• Create a formal AI governance committee to guide decision-making. • Include risk and ethics assessments at the planning stage.
DATA MANAGEMENT	• Manage data quality pipelines: cleaning, deduplication, validation. • Create centralized and accessible data repositories. • Document data lineage and maintain metadata catalogs.	• Adopt a data-centric AI approach — prioritize improving data before model tuning. • Regularly audit for bias and ensure datasets are representative and inclusive.
MODEL DEVELOPMENT	• Use reproducible and version-controlled experiments (e.g., MLflow, DVC). • Ensure fairness, explainability, and interpretability are considered during design. • Test models using diverse, real-world scenarios and edge cases.	• Choose interpretable models where possible in high-stakes domains (finance, healthcare). • Incorporate human-in-the-loop validation for critical decisions.

Ethics & Governance	• Embed responsible AI frameworks into development pipelines. • Maintain detailed documentation for audits (model cards, datasheets). • Establish clear accountability for decisions made by AI systems.	• Conduct regular ethical impact assessments. • Train all teams (technical and non-technical) on AI risks and responsible practices.
Deployment & Operationalization	• Use CI/CD and MLOps pipelines to streamline model deployment. • Containerize models and use APIs for flexible integration. • Plan for scalable infrastructure early (cloud-native preferred).	• Simulate production conditions during pre-deployment testing. • Set rollback strategies and monitor key SLAs (latency, availability, accuracy).
Monitoring & Maintenance	• Continuously track model performance, drift, and input anomalies. • Set up real-time alerts for critical issues (e.g., sharp performance drop). • Schedule regular retraining using new labeled data.	• Integrate feedback loops from users and systems for continuous improvement. • Treat AI models as evolving products, not one-time deliverables.
Documentation & Communication	• Maintain complete documentation throughout the lifecycle (from data to decisions). • Use model cards and decision logs to capture rationale and assumptions. • Communicate model limitations transparently with stakeholders.	• Enable knowledge sharing across teams through centralized wikis or dashboards. • Include non-technical summaries for leadership and compliance teams
Sustainability & Scalability	• Optimize models and pipelines for energy and computer efficiency. • Favor lighter models unless complexity is justified by impact. • Use cloud resources responsibly — consider carbon-aware training.	• Track and report the environmental cost of AI initiatives. • Design modular systems that allow reusability and component sharing across teams.

7) CONCLUSION

AI Lifecycle Management is essential to unlock the full potential of AI while minimizing risk and maximizing impact. By adopting structured engineering processes, leveraging the right tools, and fostering cross-functional collaboration, organizations can build robust, ethical, and scalable AI systems.

Managing Ai risks and implementing Responsible AI must be the top consideration for AI Lifecycle Management.