CIO Checklist for Safer and More Scalable AI Application Delivery

The VMware Tanzu AI Solutions team has designed this checklist for IT leaders that want to safely deliver AI applications in their organizations. Leaders who have experienced shadow AI or have delivered AI POCs should already have most of the working knowledge to answer these questions. However, if you are just starting out, we recommend investing some time to develop this material up front. Executives can also use this checklist to develop elements of an AI business case for their Board of Directors and measure ongoing success.

This checklist offers the essential guidance on the roles, requirements, and processes for securely delivering AI applications.

Strategy and Planning	
AI Strategy Alignment: Develop a clear AI strategy aligned with the company's overall business goals.	☐ Define primary business goal ☐ Define secondary business goal ☐ Document key performance indicators ☐ Identify Owners / Stakeholders ☐ Formalize reporting templates / cadence

Use Case Identification: Identify specific business areas where AI can deliver measurable value.	☐ Specify new / existing application ☐ Identify functional use case(s) - e.g. queries to KB articles, e-commerce conversion assistants, customer support agent, insurance claims workflow ☐ Define AI application target pattern or type - e.g. agentic AI, retrieval-augmented generation (RAG), or Generative AI (GenAI) app, etc.
Business Case Development: Establish compelling business cases for AI initiatives.	☐ Define problem statement ☐ Document cost-benefit analysis ☐ Perform risk assessment analysis ☐ Develop engineering execution plan
AI Readiness Assessment: Evaluate the organization's readiness for AI adoption, including data, infrastructure, and skills.	☐ Specify automated AI readiness assessment tools (in house / new tool?) ☐ Perform AI maturity model assessment ☐ Catalog in house platforms ☐ Catalog existing AI apps ☐ Collect vetted / certified AI models list ☐ Document POCs performed and learnings

Data Governance: Establish clear data governance policies, including data provenance, data privacy, and security requirements.	☐ Ascertain industry requirements
	☐ Identify regulation requirements
	  ☐ Data / model residency?
	  ☐ Data privacy?
	  ☐ Data protection?

	☐ Sovereign cloud? ☐ Private cloud? ☐ On premise infrastructure?
Budget Parameters: Select models for testing and production phases that fit your organization's budget requirements.	☐ Identify budget oversight owner ☐ Define testing budget ☐ Define app operations budget ☐ Specify the test / production model pricing structure ☐ Optimize models costs on an ongoing basis through techniques like model swapping and model distillation
Implementation	
Environment, Application & AI Model Security: Ensure a secure environment for AI deployment, including best practices for infrastructure, software, and model controls.	☐ Replicate secure coding practices and continuously monitor vulnerabilities. ☐ Proscribe use of industry-standard security measures such as encryption, authentication and access control ☐ Consider AI model gateways or proxies for safe ingress & egress
AI Tool Selection: Select and evaluate AI models and platforms, considering scalability, flexibility, developer experience and regulatory compliance.	AI-Ready Dev Frameworks / languages: ☐ Utilize polyglot vs. specific language framework? ☐ Utilize accelerators vs. coding assistants? ☐ Utilize cloud provider-specific frameworks? Platforms:

	☐ DIY vs. Platform-as-a-Service (PaaS) environments? ☐ Preconfigured vs. custom environments? ☐ Allow ticketed vs. self-service model access? ☐ Use coding advisors? ☐ Use coding assistants?
Data Processing and Transformation: Ensure the necessary data infrastructure, pipelines, storage and compliance solutions are in place.	☐ Ensure a unified data architecture supporting structured, semi-structured, and unstructured data for AI workloads ☐ Confirm infrastructure is future-ready to handle expanding data volumes and AI model requirements ☐ Audit your current data and storage and catalog your confidential / sensitive data exclusions ☐ Expand your data governance and data protections approach and specify data sources and acceptable use policies ☐ Design AI data pipelines against acceptable use policies (use case dependent) ☐ Validate availability of reliable, real-time and batch data ingestion pipelines across critical data sources ☐ Verify that your data governance complies with local regulations for AI ☐ Ensure you can redact confidential data / identify intelligent data substitutions to protect intellectual property ☐ Develop an incident response process in the case of accidental leakage ☐ Select unified tools, reduce integration burdens in order to evolve apps to new AI/ML models, workloads, and architectures.
Scalability and Performance: Evaluate AI solutions for	☐ Define governance in terms of budget and performance

scalability and performance to meet more rapid iteration needs for AI applications.	☐ Define how to scale the following while maintaining continuous updates for AI models: ☐ App runtime provisioning ☐ Database provisioning ☐ Model provisioning ☐ Model Observability ☐ Eval and feedback hooks ☐ Rate limiting, cost controls & accounting ☐ Binding, secrets management, credential rotation ☐ AI risk assessment (includes auths, security, devex)
Training and Education: Provide training and education to employees on AI tools and responsible usage.	☐ Formulate an AI "Center of Excellence" ☐ Train employees on AI best practices / security ☐ Define a plan to continuously train your teams on security measures, explainability techniques and data protection protocols
Risk Management and Ethics:	
Legal Compliance: Ensure compliance with relevant data protection regulations and other legal requirements.	☐ Catalog and track model versions and environment histories ☐ Enable compliance auditing with replay capabilities ☐ Implement model audits (automated or multi-tier) for explainability / accountability ☐ Implement explainability tools and reporting
Ethical AI Practices: Establish ethical guidelines for AI development and deployment, including bias mitigation and	☐ Form an "AI Ethics Council" to steer AI practices ☐ Identify training data provenance for models ☐ Create bias monitoring / bias mitigation plan

fairness.	☐ Implement a PII redaction and content safety strategy
Governance and Operations:	
AI Governance Framework: Establish a clear AI governance framework with defined roles and responsibilities.	☐ Define roles and responsibilities for managing AI models and their outputs. ☐ Define processes for handling potential issues or incidents from both a personnel and technology standpoint. ☐ Implement explainability and transparency and interpretability techniques with your models so model decision can be explained
Risk Tolerance: Understand the company's AI risk profile and set or approve the tolerance for AI risks.	☐ Assess the risks specific to your organization, including ☐ data sources used ☐ potential biases ☐ security threats ☐ Create an AI model inventory for all AI models in use, their purpose and the associated risks ☐ Understand the potential risks associated with each AI application and methodology
Continuous Monitoring: Implement mechanisms for continuous monitoring and evaluation of AI systems.	☐ Traditional service availability factors: saturation, response times, errors ☐ AI evaluation hooks - logging inputs and outputs (noting risk of private information in logs) ☐ Input guardrails - e.g. jailbreak detection ☐ Output guardrails - e.g. content safety, PII detection ☐ User feedback safely stored for model update training

Regular Reviews: Conduct regular reviews of AI initiatives and governance frameworks.	☐ Identify model and application audit tooling ☐ Ensure the Board of Directors receives scheduled updates

This checklist aims to stimulate internal discussions regarding the necessary personnel, actions, and methodologies needed for securely deploying AI applications, but is, by no means, exhaustive. To streamline and automate implementation, risk mitigation, governance and operations portions of this checklist, you may want to consider investigating **VMware Tanzu AI Solutions available in Tanzu Platform 10 and above**.

What is VMware Tanzu AI Solutions

Tanzu AI Solutions is a set of capabilities in the Tanzu portfolio of products that provides an AI-ready development framework and a cloud-native application platform, specifically engineered to expedite the secure deployment of AI-embedded applications. It streamlines the development process by abstracting complexities, allowing developers to seamlessly build, bind, deploy, and scale AI applications, treating them like any other application. This empowers development teams with the tools needed to innovate while upholding robust security standards.

For enhanced privacy and performance, Tanzu AI Solutions can be integrated with VMware Private AI Foundation, powered by NVIDIA. This integration facilitates the hosting of AI models on GPU infrastructure, significantly boosting AI workload efficiency. The combined solution accelerates time-to-market, optimizes infrastructure performance, enhances scalability, and enables development teams to rapidly deliver cutting-edge AI-embedded applications.

To learn more - please reach out to your Tanzu sales representative.