sonatype

CHECKLIST

# AI-First Software Delivery Readiness

## AI-First Delivery Creates a New Operating Reality:

Velocity increases. Risk scales. Governance has to keep up.

**SPEED**

More code, components, artifacts, and decisions

**RISK**

More exposure from malicious, vulnerable, or unapproved packages

**CONTROL**

More need for automated governance, visibility, and SBOM readiness

AI is having a transformative effect on software delivery, particularly in the productivity gains it offers. When used effectively, AI can convert software delivery from a business constraint into a business accelerator. But as development velocity increases, so does the volume of code, components, artifacts, and decisions flowing through the software supply chain.

That creates new executive challenges, including how to realize the benefits of AI without compromising security, compliance, resilience, or trust. AI-assisted development can help teams move faster, but it can also introduce risk faster. It can recommend vulnerable dependencies, pull in malicious packages, generate insecure code, expand the attack surface, and create audit gaps that are difficult to see until they become business problems.

For leaders responsible for innovation, risk, and operational performance, readiness means having AI governance and visibility to keep pace.

We've put together this AI readiness checklist to help organizations evaluate whether they are prepared to scale AI-first software delivery. It examines the core capabilities needed to protect software inputs, guide developer and AI-agent decisions, enforce policy, manage open source risk, maintain SBOM and compliance readiness, and measure whether AI is improving delivery outcomes without increasing exposure.

### What is AI-First Software Delivery Readiness?

AI-first software delivery readiness is an organization's ability to safely scale AI-assisted software development while maintaining AI software supply chain security, open source governance, compliance, SBOM visibility, and operational control.

## AI Changes Software Supply Chain Risk

This isn't an entirely new software supply chain problem, but it is accelerating one that organizations are already struggling to control. As developers and AI-assisted coding tools consume open source dependencies faster than ever, the window to identify risky, outdated, or malicious components is shrinking. AI agents can recommend, install, or even introduce packages without the same level of human scrutiny, increasing the risk of dependency confusion, typosquatting, and other malicious package attacks.

At the same time, AI-generated code can expand application attack surfaces by producing insecure patterns, pulling in unnecessary libraries, or obscuring where vulnerable components enter the development lifecycle. This growing complexity is colliding with rising regulatory pressure around SBOMs, software transparency, and third-party risk management.

To keep up, governance has to move at machine speed, continuously evaluating components, enforcing policy automatically, and generating trusted software inventories.

# 8 READINESS QUESTIONS FOR AI-FIRST SOFTWARE DELIVERY

## 01 Do you have a trusted foundation for AI-scale software delivery?

AI-first development increases the number of components, containers, models, builds, and artifacts moving through your software supply chain. Without a trusted foundation, it becomes harder to know what is being used, where it came from, who approved it, and whether it is safe to ship.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ Centralize and govern software components, containers, and AI/ML models
- ☐ Maintain end-to-end traceability across artifacts, applications, and teams
- ☐ Connect artifact management with policy, security, and compliance workflows
- ☐ Ensure developers and AI-assisted workflows use approved components
- ☐ Scale repository infrastructure as build volume and dependency usage increase
- ☐ Verify artifact provenance before components are used in builds


### HOW SONATYPE HELPS

Sonatype Nexus Repository provides the trusted foundation for modern software delivery by helping organizations store, manage, and govern software components, containers, and AI/ML models at scale. As AI increases delivery speed and software volume, it also acts as the system of record for the artifacts and metadata teams need to build with confidence.

## 02 Can you stop malicious components before they enter development?

AI coding assistants and agents can recommend dependencies quickly, but they don't always know whether a package is secure, approved, maintained, malicious, or compliant with company policy. If malicious components enter development unchecked, they can create downstream rework, build failures, security exposure, and production risk.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ Quarantine suspicious components before they reach developers or builds
- ☐ Prevent vulnerable or policy-violating packages from entering repositories
- ☐ Guide developers toward safer choices without adding manual review
- ☐ Block malicious open source packages before download
- ☐ Protect both Nexus and non-Nexus repositories

### HOW SONATYPE HELPS

Sonatype Firewall blocks malicious, vulnerable, and policy-violating components at the point of entry, while Sonatype Nexus Repository provides the trusted foundation for managing approved components. Sonatype Guide extends protection into developer and AI-agent workflows by helping teams avoid risky dependency decisions before they create downstream rework.

## 03 Can developers and AI agents make trusted dependency decisions?

AI can help teams write code faster, but faster dependency selection doesn't translate into better dependency selection. Developers and AI agents need access to trusted intelligence at the moment choices are made, not only after a scan fails later in the pipeline.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ Help developers choose safer, healthier, and more appropriate dependency versions
- ☐ Reduce technical debt caused by outdated or poorly maintained components
- ☐ Support secure development without requiring every developer to become a security expert
- ☐ Provide AI workflows trusted open source intelligence
- ☐ Provide guidance before risky packages are introduced

### HOW SONATYPE HELPS

Sonatype Guide helps developers and AI agents make better open source decisions with trusted dependency intelligence and automated guidance. It supports safer component selection, faster remediation, and reduced technical debt, helping organizations turn AI-assisted development into productivity gains rather than future rework.

## 04 Can you enforce open source policy without slowing delivery?

Yes, but it doesn't happen by itself. As AI accelerates software delivery, manual governance can no longer keep up. Teams are writing more code, using more dependencies, and generating more policy violations across more applications. Without automated enforcement built into the SDLC, security and engineering teams face more risk, more remediation work, and less confidence in what is being shipped.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ Apply security, license, and quality policies consistently across teams
- ☐ Define enforcement actions based on risk level and business context
- ☐ Track policy exceptions, waivers, and approvals
- ☐ Enforce policy in IDE, source control, build, repository, and release workflows
- ☐ Provide clear explanations and remediation paths when blocked

### HOW SONATYPE HELPS

Sonatype Lifecycle helps organizations automate open source governance across the SDLC. It enables teams to enforce policy, monitor risk, manage exceptions, and maintain visibility without relying on manual review. Lifecycle helps security and engineering teams scale governance at the speed of AI-assisted development.

## 05 Can you maintain visibility as AI increases software volume?

AI-assisted development can create more applications, more builds, more dependencies, more artifacts, and more release activity. But without centralized visibility, leaders lose confidence in what is being built, what is at risk, and where action is needed.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ See open source component usage across applications, teams, and repositories
- ☐ Prioritize risk by application context, exploitability, and business impact
- ☐ Give security, engineering, and executive teams visibility to act quickly and confidently
- ☐ Identify applications affected by a new vulnerability, malicious package, or policy issue
- ☐ Connect repository, dependency, policy, and SBOM data into a single view of software risk

### HOW SONATYPE HELPS

The Nexus One Platform brings together the intelligence, controls, and visibility organizations need to protect, guide, and govern software delivery at AI scale. Nexus Repository provides the foundation; Sonatype Firewall prevents risky components from entering; Sonatype Lifecycle governs risk across the SDLC; Sonatype Guide supports better developer and AI-agent decisions, and Sonatype SBOM Manager extends transparency and compliance visibility.

## 06 Can you prove what's in your software?

AI increases the need for software transparency. As AI-assisted development scales, organizations need to prove what components are in their software, where they came from, what risks they carry, and whether they meet compliance obligations.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ Generate, ingest, manage, and share SBOMs at scale
- ☐ Manage license obligations and compliance requirements
- ☐ Monitor SBOMs continuously as new risk emerges
- ☐ Track software inventory changes over time
- ☐ Respond quickly to customer, auditor, or regulator requests

### HOW SONATYPE HELPS

Sonatype SBOM Manager helps organizations manage software transparency and compliance at scale. It supports SBOM governance, ingestion, sharing, license management, and ongoing visibility so teams can demonstrate that AI-first delivery remains auditable, compliant, and trustworthy.

## 07 Can you reduce developer rework instead of increasing it?

AI is often positioned as a productivity accelerator, but speed gains can disappear if developers spend more time fixing AI-generated output than building new features. In fact, 67% of developers say they spend more time debugging AI-generated code than writing new code. For AI to improve software delivery, organizations need to reduce the downstream rework caused by risky dependencies, late-stage policy failures, and avoidable security issues.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ Give developers useful feedback before risky code or components are committed
- ☐ Provide specific, actionable remediation guidance rather than generic alerts
- ☐ Embed security and governance into existing development workflows
- ☐ Prevent packages from being used if they will later be blocked
- ☐ Help AI agents safely assist with dependency updates and technical debt

### HOW SONATYPE HELPS

Sonatype helps reduce avoidable rework across the SDLC. Sonatype Firewall prevents bad components from entering development, Sonatype Guide helps developers and AI agents make better dependency decisions, and Sonatype Lifecycle automates policy enforcement and remediation guidance. Together, they help teams preserve the productivity benefits of AI while reducing downstream friction.

## 08 Can you measure whether AI is improving delivery without increasing risk?

AI software delivery readiness requires proving the benefits to the organization, including faster delivery while maintaining or improving security, compliance, resilience, and control.

### CONSIDER WHETHER YOUR ORGANIZATION CAN:

- ☐ Track policy violations, blocked components, remediation trends, and dependency health
- ☐ Demonstrate faster identification, prioritization, and remediation of supply chain risk
- ☐ Connect AI adoption to outcomes such as release frequency, lead time, developer efficiency, and executive confidence
- ☐ Measure software delivery speed and overall risk posture together
- ☐ Show whether AI-assisted development reduces rework or shifts risk downstream

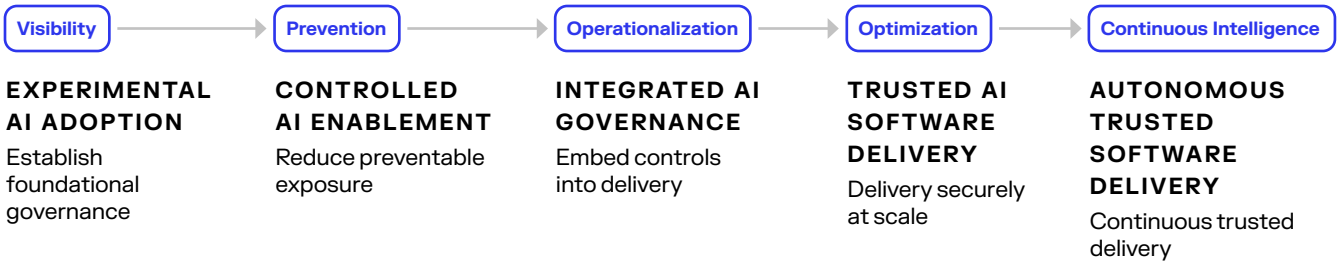
### HOW SONATYPE HELPS

Sonatype helps organizations connect software delivery speed with software confidence. Across the Nexus One Platform, teams can manage trusted artifacts, prevent risky components from entering development, govern open source policy, guide developer decisions, maintain SBOM readiness, and measure software supply chain risk. This gives leaders the visibility and control needed to understand whether AI is improving delivery outcomes without expanding exposure.

## AI-Driven Software Delivery Maturity Model

AI software delivery maturity varies widely. Some organizations are still focused on enabling AI productivity, while more mature organizations build the governance, visibility, and automation needed to sustain that productivity at scale. As software delivery accelerates, the differentiator is no longer how quickly AI can generate code. It's how confidently organizations can trust what developers and AI agents assemble.

Organizations prepared for AI-driven software delivery don't rely on manual reviews after the build. They continuously validate what developers and AI agents assemble before it reaches production. By embedding trusted component intelligence, automated policy enforcement, and continuous governance throughout the SDLC, they enable teams to innovate at AI speed without sacrificing security, compliance, or operational resilience.




## Best Practices for Trusted AI Delivery

- Centralize software artifacts, containers, and AI/ML models
- Use approved repositories and trusted artifact sources
- Standardize repository governance across teams
- Maintain traceability for components and builds
- Establish a system of record for software components
- Scale repository infrastructure to support AI-driven build volume

## Speed Creates a New Kind of Risk

As development accelerates, leaders need confidence that the code, components, artifacts, and applications moving through the software supply chain are secure, compliant, traceable, and governed.

Sonatype helps organizations close the gap between AI-first software creation and trusted software delivery. With the Nexus One Platform, teams can protect software inputs, guide developer and AI-agent decisions, automate open source governance, maintain SBOM and compliance readiness, and measure risk across the SDLC.

## Find Out Whether Your Software Supply Chain Is Ready For AI-Speed Delivery

**BOOK A PERSONALIZED DEMO**

Use this checklist to uncover where your organization has strong controls, where AI may be introducing new risk, and where manual processes may be slowing teams down. Then, meet with Sonatype to map your readiness gaps to practical next steps across artifact management, dependency protection, open source governance, SBOM readiness, and developer guidance.

Schedule a readiness assessment with Sonatype today and get a real-world look into what your organization can do to harness the potential of AI-first software delivery.

sonatype

Sonatype is the leader in AI-driven DevSecOps. As the maintainers of Maven Central and creators of Nexus Repository, Sonatype has spent two decades pioneering how the world manages and secures open source software — making Sonatype the trusted authority for modern software supply chains. With unmatched open source visibility and a unified product suite built for modern software development, Sonatype gives enterprises the intelligence and automated governance they need to harness the full potential of open source and AI. Sonatype handles the complexity behind the scenes: guiding component and model selection, blocking harmful malicious code, automating dependency and vulnerability management, and ensuring faster, more reliable builds — so developers spend more time on innovation and less time on remediation and rework. Trusted by more than 15 million developers, Sonatype helps power secure, modern software development at nearly 2,000 global organizations including 70% of the Fortune 100. To learn more about Sonatype, please visit www.sonatype.com