AIMS™ Technology FAQ

Frequently Asked Questions

For IT Leaders, Compliance Officers & Due Diligence Teams

PentEdge LLC — AI with Guardrails™

Confidential — 2026

About This Document

This FAQ addresses the most common questions from IT leaders, compliance officers, operations teams, and vendor due diligence reviewers evaluating AIMS™. Questions are grouped by topic area. For a product overview or demo, contact lisa@thepentedge.com.

1. AI DISCOVERY & MONITORING

How does AIMS™ discover AI tools without installing software on endpoints?

AIMS™ uses agentless detection via read-only API connections to your existing infrastructure. It connects to M365 audit logs, Active Directory / Entra ID sign-in telemetry, OAuth consent and permission grants, network logs, and firewall telemetry. Nothing is installed on user devices. No endpoint agent is required.

Does AIMS™ read employee conversations or access message content?

No. AIMS™ identifies tool usage at the application level only. It does not read conversations, access data content, monitor employee communications, or capture transaction details. It provides governance visibility, not surveillance.

What AI tools does AIMS™ detect out of the box?

AIMS™ includes pre-built detection and risk profiles for Microsoft Copilot, ChatGPT (OpenAI), Google Gemini, Claude (Anthropic), and other commonly used AI platforms. It also detects custom integrations and developer-built frameworks. The inventory can be supplemented manually via the UI or bulk CSV import for tools not automatically detected.

What is an AI Tool Instance?

An AI Tool Instance is one discrete AI-powered product in your environment, associated with a specific vendor and status. A single vendor can have multiple instances (for example, a vendor's customer-facing tool and their internal analytics tool would be two separate instances). Each instance is assessed independently for risk.

How are dormant tools handled?

Dormant tools (no longer actively used) remain in the governance record but are weighted at 25% in composite risk scoring versus 100% for active tools. This keeps them visible for audit purposes without inflating your overall risk posture. They are also flagged as cost-saving opportunities if associated costs remain active.

2. INTEGRATION & ARCHITECTURE

What IT infrastructure does AIMS™ require?

AIMS™ requires no special infrastructure, no elevated service account credentials, and no changes to your core banking systems. It connects via read-only APIs to your existing Microsoft 365 environment, Active Directory / Entra ID, and network telemetry sources. Ongoing IT maintenance is approximately 2–3 hours per week post-launch.

How does AIMS™ integrate with our GRC platform?

AIMS™ integrates via REST API with Archer, ServiceNow, and other GRC platforms, configurable per deployment. A structured file export is available as a fallback for institutions without a GRC platform. Integration scope is confirmed during the implementation discovery phase.

Is AIMS™ a replacement for our existing risk management systems?

No. AIMS™ is an overlay solution. It does not replace your core banking platform, enterprise risk management system, or any other existing tool. It works alongside your current architecture via API connections.

What is the implementation timeline?

Implementation follows a 90-day path: Day 30 — discovery complete, AI inventory documented, system configured. Day 60 — testing complete, team trained, governance reports generating. Day 90 — live examiner-ready documentation established, full AI tool visibility achieved. Pace is flexible with no penalties for adjustment.

How much IT time does implementation require?

Approximately 10–15 hours per week during the discovery and testing phases. Post-launch maintenance requires approximately 2–3 hours per week. The PentEdge implementation team handles the technical heavy lifting.

3. DATA SECURITY & PRIVACY

What data does AIMS™ access?

AIMS™ accesses metadata and audit logs from AI tools and your network — not customer PII, core transaction data, or conversation content. Only information necessary to maintain inventory, assess risk, and generate compliance documentation is accessed.

Where does our data stay?

Data remains in your configured environment. Nothing is extracted to shared external locations without explicit consent. Cloud deployments use dedicated tenants with no cross-institution data mixing or commingling of customer data.

What encryption and access controls are in place?

AIMS™ implements: Role-Based Access Controls (RBAC) — users see only information relevant to their role; TLS 1.2 or higher for all data in transit; AES-256 encryption for all data at rest; full audit logging of all system access and changes.

What user access levels are available?

Two roles: Bank Admin — full tool access, inventory management, and user administration. Bank User — tool access, assessment participation, and reporting (no user management). Additional role configurations are available on request.

4. REGULATORY & COMPLIANCE

Which regulatory guidance does AIMS™ align with?

AIMS™ governance outputs are structured to address AI oversight requirements from OCC, FDIC, Federal Reserve, NCUA, CFPB, FinCEN, and state regulators including NYDFS. The framework draws on SR 11-7, OCC Bulletin 2023-17, FDIC FIL-29-2024, NIST AI RMF, ECOA/FHA, UDAP/UDAAP, BSA/FinCEN, the FFIEC IT Handbook, GLBA, and CFPB Circular 2022-3.

What examiner-ready documentation does AIMS™ produce?

One-click PDF reports include: (1) AI tool inventory and classifications, (2) risk scores and risk distribution, (3) governance controls in place, (4) compliance status — DHA, NDA, VDD, RAG, (5) vendor information and due diligence status, (6) historical governance decisions and full audit trail.

What compliance documents does AIMS™ track?

AIMS™ tracks Data Handling Agreements (DHA), Non-Disclosure Agreements (NDA), Vendor Due Diligence documentation (VDD), and RAG compliance status across five states: Compliant, Validation in Progress, Partial, Non-Compliant, and Not Assessed.

How does the human-in-the-loop governance model work?

AIMS™ alerts your team when governance action is needed — tool review overdue, compliance deadline approaching, high-risk tool detected, or vendor update received. Your team reviews the alert and decides the appropriate response: Resolve, Acknowledge, or Defer. All decisions are recorded in an immutable audit trail. No autonomous action occurs without human review and approval.

How is the audit trail maintained?

The immutable audit log records: who took the action, when it occurred, what system fields changed, what action was taken, and the user's reasoning and notes. This provides full traceability for compliance and examination purposes. Data is retained per your institution's configured retention policy.

5. VENDOR DUE DILIGENCE & SUPPORT

What risk dimensions does AIMS™ assess for each tool?

Each AI tool is scored across five dimensions: Regulatory Risk (compliance and examination exposure), Operational Risk (process disruption potential), Model Risk (accuracy, reliability, and bias), Vendor Risk (vendor security, stability, and reliability), and Fair Lending Risk (discrimination or unfair lending potential).

How does the three-stage risk scoring model work?

Stage 1 — Inherent Risk: baseline assessment across the five dimensions (0–100 scale). Stage 2 — Mitigant Controls: assessment of control effectiveness across six categories (Policies, Human Oversight, Monitoring & Logging, Vendor Due Diligence, Training, and Audit). Stage 3 — Residual Risk: Inherent Risk minus mitigation effectiveness, yielding a final band of Low, Medium, High, or Critical.

What post-implementation support is included?

Post-implementation support includes: a dedicated named contact for your institution (not a ticketing queue), direct communication channels, regular check-ins at your cadence, and staff training and documentation. Implementation is flexible with no penalties for adjusting pace — quality is prioritized over speed.

What if AIMS™ flags something incorrectly?

All flags are reviewed by your team before any action is taken. AIMS™ documents observations and generates alerts — it does not automatically remediate or take autonomous action. Your team has full authority over every governance decision.

Can implementation pace be adjusted?

Yes. There are no penalties for adjusting implementation pace. The team works with your organization to find a sustainable rhythm. Go-live occurs only when both teams are confident the system is properly configured and tested.

Questions not answered here?

Contact Lisa Pent and the PentEdge team directly. We're happy to walk through any technical requirement, integration question, or due diligence item your team needs answered before a demo.

lisa@thepentedge.com • thepentedge.com