TEMPLAR shield

ENTERPRISE ASSET MANAGEMENT FLIGHTPATH (EAM)

Created by:
Nicholas Friedman
CEO & Founder of Templar Shield

Section 1:

Enterprise Asset Management (EAM) Flightpath – Executive Summary

Problem Statement

Enterprises today face fragmented asset visibility across three critical domains:

- **IT Assets** (endpoints, infrastructure, software, cloud services)
- **OT Assets** (industrial control systems, sensors, SCADA/PLC devices)
- **AI Assets** (models, datasets, prompts, agents, use cases)

Each of these domains often operates in silos, managed by different teams, with separate tools and compliance frameworks. This fragmentation results in:

- **Inconsistent inventories** and "shadow assets" (untracked endpoints, rogue AI deployments, or legacy OT devices).
- **Inefficient operations**, with duplicated processes for lifecycle management, patching, and compliance.
- **Elevated risk exposure**, from unmonitored vulnerabilities, unmanaged access rights, or AI bias and drift.
- **Regulatory pressure**, as global standards (NERC CIP, IEC 62443, EU AI Act, ISO 55000) mandate integrated oversight across IT, OT, and AI ecosystems.

Recommendation: Integration Through a Unified Flightpath

To address these gaps, we recommend adopting an Enterprise Asset Management (EAM) Flightpath built on ServiceNow IRM, SecOps, ITOM, HAM/SAM, OTAM, and AI Control Tower.

The EAM Flightpath provides:

- **Unified Visibility**: A single CMDB extended to IT, OT, and AI assets.
- **Lifecycle Governance**: Standardized onboarding, policy alignment, and automated workflows.
- **Risk-Based Operations**: Coordinated vulnerability, patch, and incident response across domains.
- **AI-Aware Oversight**: Inclusion of AI models, datasets, and prompts as governed enterprise assets.
- **COE Leadership**: A permanent Enterprise Asset Governance Center of Excellence to sustain integration.

The Flightpath Approach

Delivered in six structured phases over ~24 months, the EAM Flightpath ensures controlled maturity progression:

1. **Visibility & Inventory** – Unified CMDB across IT, OT, and AI.
2. **Lifecycle & Policy Foundation** – Standardized workflows and compliance mapping.
3. **Vulnerability & Patch Governance** – Risk-based remediation and monitoring.
4. **Incident & Risk Response** – Coordinated, cross-domain security and resilience.
5. **Posture & Access Governance** – Identity, access, and compliance enforcement.
6. **Oversight & Future-Proofing** – Real-time dashboards, regulatory reporting, and a Governance COE.

Overall Benefits to the Customer

By following the EAM Flightpath, enterprises will achieve:

- **Single Source of Truth** – Elimination of duplicate or "ghost" assets.
- **Operational Efficiency** – Automation reduces manual effort and accelerates response times.
- **Integrated Compliance** – Always-on alignment with IT, OT, and AI regulatory standards.
- **Risk Reduction** – Faster MTTR for incidents, fewer compliance gaps, and reduced attack surface.
- **Future-Proof Governance** – AI, IT, and OT asset oversight embedded into daily operations.
- **Board-Level Trust** – Transparent, auditable dashboards and reports for executives and regulators.

This positions the customer to not only reduce cost and risk, but also to scale innovation responsibly—turning integrated asset management from a compliance burden into a competitive advantage.

Section 2:

Here's a structured deep-dive into the four domains you asked me to explore—ITAM/ITOM (with ServiceNow + Tanium), HAM/SAM, OTAM/OTOM, and AI/Enterprise Asset Management—followed by a synthesized Enterprise Asset Management (EAM) Flightpath that integrates IT, OT, and AI assets, using your IRM, SecOps, and AI Control Tower flightpath docs as reference points.

1. IT Asset Management (ITAM) and IT Operations Management (ITOM)

ServiceNow ITAM:

- Automates the asset lifecycle from procurement to retirement.
- Modules: Hardware Asset Management (HAM), Software Asset Management (SAM), and Cloud Insights.
- Benefits: optimized license usage, reduced cost of unused assets, compliance with vendor contracts, alignment with CMDB (Configuration Management Database).

ServiceNow ITOM:

- Provides **asset discovery and visibility** (via Service Graph Connectors, Discovery, and Service Mapping).
- Key: integrates infrastructure, applications, and cloud workloads into a unified CMDB baseline.
- Outcomes: service-aware operations, proactive event and anomaly detection, automated remediation.

Tanium IT Asset Management:

- Focuses on real-time endpoint visibility and patch/configuration compliance.
- Key differentiator: "converged endpoint management"—scales to millions of endpoints, providing instant query and action.

ServiceNow + Tanium Integration:

- Tanium provides real-time discovery and compliance posture for endpoints.
- ServiceNow consumes this into ITAM/ITOM modules for unified CMDB, asset lifecycle workflows, and risk-based vulnerability response.
- Example: A missing software patch identified by Tanium can auto-create a ServiceNow Vulnerability Response ticket, tied to ITAM asset records.

2. Hardware Asset Management (HAM) & Software Asset Management (SAM)

HAM (Hardware Asset Management):

- Automates receiving, provisioning, and retirement of devices.
- ServiceNow HAM integrates with procurement, finance, and lifecycle management to eliminate ghost assets and enforce warranty/lease terms.
- In the EAM context, HAM extends to IoT/OT hardware with asset classes in the CMDB.

SAM (Software Asset Management):

- Normalizes software titles, reconciles licenses, and automates renewal/true-up decisions.
- Integrates with HAM and ITOM for compliance and spend optimization.
- Advanced SAM also includes SaaS and cloud license management.

3. OT Management (OTM, OTOM, OTAM)

From the SecOps Flightpath

14 - SecOps Flightpath v.1 1:

- **Phase 1**: Asset visibility & unified CMDB—ITOM Discovery + OTAM + OTM (with integrations to Tenable.ot, Claroty, ForeScout, Nozomi).
- **Phase 2**: Integrated IT/OT Operations—incident/change management, FSM dispatch for plant-level fixes.
- **Phase 3**: Vulnerability & Patch Governance—coordinated IT/OT vulnerability remediation.
- **Phase 4–6**: Incident Response, Security Posture Control, and Identity/Access Governance.

Key Outcomes:

- Unified CMDB extended to OT.
- Reduced MTTR (mean time to resolve) for OT incidents.
- Compliance with OT frameworks (NERC CIP, IEC 62443).

Operational Technology Asset Management (OTAM):

- Specialized for ICS/SCADA devices, sensors, and PLCs.
- Requires passive discovery (to avoid downtime).
- Maps asset dependencies to critical services.

4. AI Asset Management (AI Control Tower, AI Inventory)

From your AI Control Tower Flightpath:

- **AI Inventory/Discovery**: Catalogs models, prompts, datasets, agents in CMDB.
- **AI Lifecycle Management**: Policy-based workflows for approval, deployment, monitoring, retirement.
- **AI Risk & Compliance**: Alignment with NIST AI RMF, EU AI Act, ISO/IEC 42001.
- **Prompt Governance**: Role-based access to AI prompts, libraries, and compliance guardrails.
- **AI Incident Response**: Linking bias, drift, hallucinations, or prompt injection attacks to SecOps workflows.

Outcomes:

- 30%+ increase in AI asset visibility.
- 80% reduction in audit prep time (automation).
- Unified oversight for boards and regulators.

5. Enterprise Asset Management (EAM) — Integrated Flightpath

Phase 1: Asset Visibility & Unified Inventory (Months 0–4)

- **IT**: ITOM Discovery + Tanium endpoint visibility.
- **OT**: OTAM + OTM passive discovery via Claroty/Tenable/Nozomi.
- **AI**: AI Control Tower inventory of models, datasets, prompts.
- Unified CMDB extended with IT, OT, AI classes under ServiceNow CSDM.
- Outcomes: single source of truth for all enterprise assets.

Phase 2: Lifecycle & Policy Foundation (Months 5–8)

- HAM/SAM integrated with procurement, finance, and compliance.
- OT lifecycle governance for industrial devices (procurement → retirement).
- AI lifecycle governance with approval workflows (deployment, updates, retirement).
- Outcomes: standardized asset onboarding, policy-driven control library, mapped to global frameworks.

Phase 3: Vulnerability, Compliance & Patch Governance (Months 9–14)

- IT: Risk-based CVE patching (Tanium + VR).
- OT: Coordinated patch governance (with FSM dispatch).
- AI: Continuous control monitoring (fairness, drift, explainability).
- Outcomes: reduced risk exposure across IT/OT/AI.

Phase 4: Incident & Risk Response (Months 15–18)

- IT: ServiceNow SIR + SOAR for endpoint and infra threats.
- OT: OT incident correlation with IT workflows.
- AI: AI-specific incident triage (bias, hallucinations).
- Outcomes: unified response across IT, OT, and AI ecosystems.

Phase 5: Posture & Access Governance (Months 19–22)

- IT/OT: Security Posture Control (SPC) + IAM/IGA for systems and operators.
- AI: Prompt governance, SoD enforcement, human-in-the-loop controls.
- Outcomes: continuous compliance, identity-risk reduction.

Phase 6: Oversight, COE & Future-Proofing (Months 23–26)

- Launch Enterprise Asset Governance Center of Excellence (COE).
- Real-time dashboards: IT asset health, OT plant posture, AI compliance scores.
- Regulatory reporting (NERC CIP, EU AI Act, ISO 55000 for EAM).
- Outcomes: integrated, resilient, and auditable EAM program—scalable across industries.