nowvia

Reimagining IT Operations in the Era of AI and Agentic AI

Not an option anymore but a genuine necessity

Operational excellence is not something organizations buy. It is something they architect. And, achieving excellence in IT operations management requires an architectural foundation rather than incremental tooling.

In this paper, we examine the extent to which ServiceNow solutions help organizations to evolve their IT operations management (ITOM) from tool-centric monitoring to a more graph-based, workflow-driven operating model, where ServiceNow functions as the system of record, experience layer, and execution plane for AI and agentic operations.

At the foundation of this model is a well-hydrated Configuration Management Database (CMDB) that is aligned to the Common Service Data Model (CSDM), acting as a knowledge graph and digital mirror of the organization, enabling AI, automation, and agentic workflows to operate safely, contextually, and at scale.

Need of the Hour

For years, a siloed IT department managed to exist and hold its specialized fort but not anymore. Gen AI and agentic AI are compelling organization leadership to now consider **technology strategy as an integral part of their business strategy.** And while operational efficiency and cost optimization are strong drivers for AI adoption,[1] organization leaders want their AI-based technology strategy to unlock revenue streams, innovation, shareholder value and more.[2]

This aspiration calls for rethinking and rewiring the IT operating model for the age of AI—one that is built around an interconnected knowledge graph of all enterprise data workflows, models that can reason and transform data into action, and autonomous agents that are able to solve problems with minimal human input.[3]

For organizations with a keen eye on the future, this will be a well-planned journey of transition (from "as is") to transformation into an organization that is driven by AIOps, automated and autonomous workflows as well as continuous and seamless integration and delivery pipeline. Moreover, as organizations leverage the power of AIOps to revolutionize their IT operating models, they will need to have the expertise to take proactive measures to mitigate potential risks associated with data quality, integration and compatibility, skills, ethics and privacy, compliance, and more.[4]

Undoubtedly, organizations will need to move way beyond mere technology upgrades, if they are to reap the full benefits of AIOps and see a clear ROI. In fact, this transformation will require the organization leadership to have the same mindset as that when we moved from steam to electricity, requiring the reconfiguration of production lines, redesigning of workflows, and a conscious decision to invest in new infrastructure and workforce reskilling.[5] Moreover, many organizations that have invested in monitoring, observability, AIOps, and automation are struggling to translate these investments into consistent operational outcomes.[6] Mean time to resolution remains high, service impact is often unclear, and AI initiatives frequently fail to move beyond isolated pilots.

In this paper, we examine the extent to which ServiceNow solutions [7] help organizations to evolve their IT operations management (ITOM) from tool-centric monitoring to more a graph-based, workflow-driven operating model, where ServiceNow functions as the system of record, experience layer, and execution plane for AI and agentic operations. At the foundation of this model is a **well-hydrated Configuration Management Database (CMDB) that is aligned to the Common Service Data Model (CSDM),** acting as a **knowledge graph and digital mirror of the organization,** enabling AI, automation, and agentic workflows to operate safely, contextually, and at scale.

Granular Problems Bubbling up to the Surface

Despite advancements in tooling, most enterprises encounter the same structural challenges.

Signal Proliferation Without Context: Modern IT environments generate a vast volume of:

Metrics, logs, and traces

Events from infrastructure, applications, and cloud platforms

Alerts from multiple observability and AIOps tools

While telemetry quality has improved, these signals often lack a shared model that explains **what they relate to, what they impact, and why they matter** from a service or business perspective.

CASE IN POINT

Business Problem:

A major global bank had millions of monitoring events every month from dozens of tools. IT operations teams felt overwhelmed by the noise and had to manually correlate incidents, leading to duplicate tickets and slow, reactive response. As a result, the bank experienced high Mean-Time-To-Restore (MTTR) and Site Reliability Engineering (SRE) burnout as critical issues were buried in irrelevant alerts.

Solution:

By deploying an AIOps event correlation platform, the bank compressed millions of raw alerts into actionable incidents, reducing alert noise by ~50%. It achieved a 35% faster detection Mean-Time-To-Detect (MTTD) and 43% faster recovery (MTTR), translating to significantly shorter outages.

Business Impact: With great efficiency in incident management, the bank reported a 4× ROI within the first year.[8]

CMDB Exists but Is Not Operationalized: In many organizations:

CMDBs are partially populated or outdated

CI relationships are incomplete or inaccurate

Ownership, lifecycle state, and accountability are unclear

CMDB is disconnected from day-to-day operations

As a result, CMDB is perceived as a compliance artifact rather than an operational foundation.

CASE IN POINT

Business Problem:

Rapid expansion and mergers left the hospital network's CMDB at Wellstar Health System, incomplete and unreliable. Many configuration items (CIs) were outdated or lacked proper relationships (that is, there were no service maps). Hence, IT operations teams couldn't trust the CMDB during incident triage or change planning. Moreover, the disjointed data led to poor change impact analysis and slower incident resolution, contributing to unplanned downtime in clinical applications.

Solution:

Wellstar decided to make CMDB a trusted asset for proactive IT support rather than a static record-keeping tool. To achieve this goal and ensure the CMDB served as a single source of truth, the hospital overhauled its CMDB with automated ServiceNow Discovery and data cleanup. This resulted in 86% accuracy in CMDB data and IT operations teams gained end-to-end visibility into their IT estate. Plus, major incident response times dropped by 25%, and root-cause analysis that used to take 30 days came down to just 4 days.

Business Impact: By eliminating legacy configuration blind spots, Wellstar was able to prevent outages and saved over $500,000, annually in efficiency gains.[9]

Service Mapping Is Static in a Dynamic Environment: Traditional service mapping approaches struggle in environments characterized by:

Ephemeral cloud resources

Containers and microservices

CI/CD-driven change velocity

Without continuously maintained service context, impact analysis, root cause analysis, and prioritization remain manual and error-prone. Today's dynamic business environment demands the use of modern discovery approaches such as pattern-based discovery, tag-based cloud discovery, Kubernetes and container discovery and continuous service mapping in CI/CD environments.

It is a fact that security and/or compliance blind spots due to incomplete asset and service mapping has a negative impact on an organization's reputation, brand and competitive position in the market.[10]

CASE IN POINT

Business Problem:

A top private bank in India with 100+ branches suffered from fragmented, siloed asset and lack of service mapping. Since its IT systems and facility infrastructure were tracked in separate tools, there were many blind spots. Furthermore, the bank's CMDB and documentation were incomplete, resulting in regulatory audit gaps.

Solution:

The bank implemented ServiceNow IT Operations Management with automated Discovery and Service Mapping to unify its CMDB, thereby providing a single pane of glass view of all IT and non-IT assets. Within 6 months, the bank achieved 96% accurate asset registry, 3x faster incident resolution, and 80% fewer audit escalations.

Business Impact: Seamless business operations, better cross-team coordination and resource utilization, and robust regulatory compliance.[11]

AI and Automation Lack a Reasoning Framework: Organizations increasingly adopt AI, GenAI, and automation within operations. However, outcomes remain inconsistent because AI systems lack:

Structured representations of the enterprise

Explicit relationships and dependencies

Business context and constraints

Governance mechanisms for execution

Without these elements, AI cannot reason effectively, and agentic systems cannot operate safely at scale. Where organizations have paid attention to these aspects, they have experienced impressive business outcomes.

CASE IN POINT

Well aware of the pitfalls of relying on reactive firefighting, Commerzbank decided to embrace an AI-augmented autonomous operations initiative.

By integrating real-time dependency mapping into its CMDB and enforcing governance around automated actions, Commerzbank gave its AI the knowledge and guardrails needed to operate as a trusted "virtual operator."

Business Impact: An order-of-magnitude drop in incident volume and resolution time—70% reduction in major incidents and 96% faster MTTR – from 30 hours to 1 – as part of its journey toward ticket-free IT operations. When AI is supported by a rich reasoning framework, IT operations can become predictive and self-healing without sacrificing safety or reliability.[12]

To address the above challenges in the AI and agentic era, businesses need to evolve their ITOM along three dimensions:

From raw data to operational knowledge

From alerts to service-centric understanding

From automation scripts to governed agency

This evolution requires an architectural foundation rather than incremental tooling changes. This is precisely what ServiceNow's CMDB provides, and is our focus in the next couple of sections of this paper.

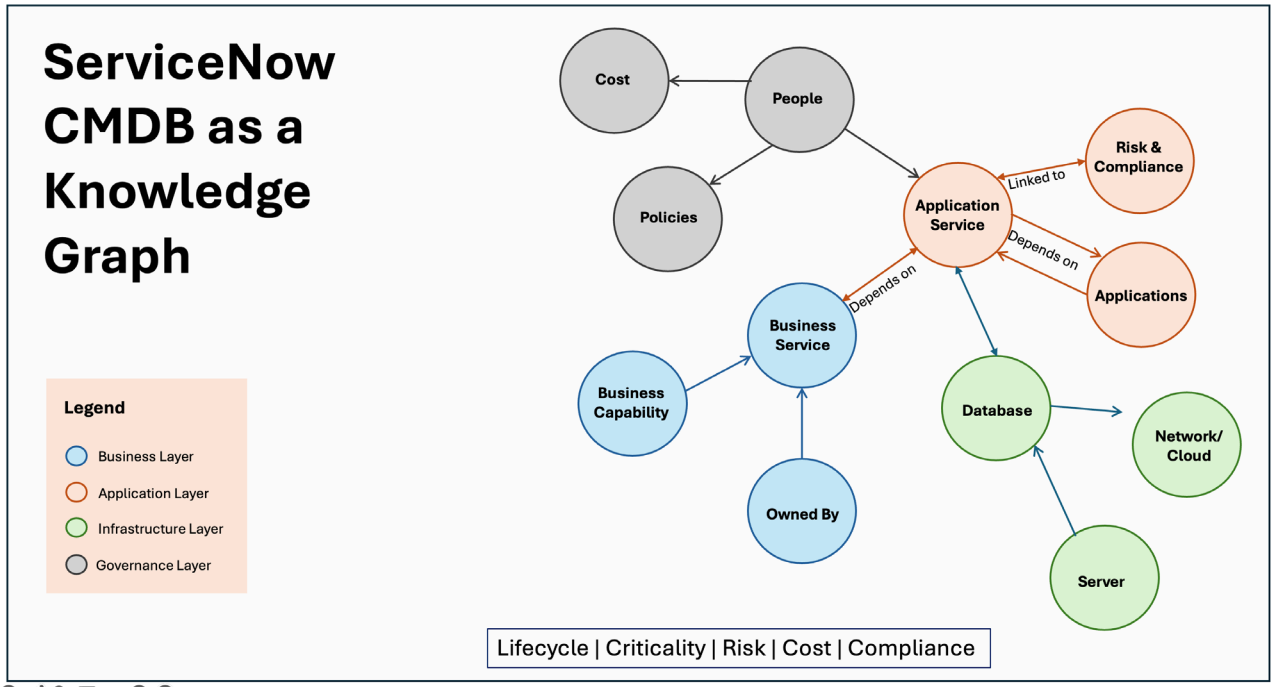
CMDB as a Knowledge Graph and Digital Mirror

ServiceNow CMDB—aligned to Common Service Data Model (CSDM)—is more than a configuration repository. It functions as a knowledge graph with:

Nodes: Assets, applications, services, business capabilities and people.

Edges: Dependency, containment, ownership and impact.

Attributes: Lifecycle state, criticality, risk, cost and compliance.



When hydrated and governed correctly, this graph becomes a digital mirror of the organization's operational environment.

Knowledge graphs are essential to AI and agentic systems but they are only as good as their underlying data with interconnected systems across the enterprise. ServiceNow's CMDB knowledge graph provides:

Structure for reasoning	Relationships for inference	Context for prioritization	Constraints for safe execution

Without such a robust knowledge graph, AI produces insights without accountability, agents act locally rather than systemically, and automation amplifies risks instead of reducing them.

CSDM as the Semantic Backbone

In the era of AI, semantic consistency is essential, and Common Service Data Model (CSDM) provides that consistency. This consistency is required for aligning infrastructure to applications, applications to business services, and services to outcomes. Furthermore, CSDM enables:

Shared vocabulary across ITSM, ITOM, ITAM, Risk and security.

Predictable traversal of the knowledge graph.

Reusable logic for AI, analytics and automation.

From Infrastructure to Business Context

In an agentic operating model, service mapping is not optional—it is foundational.

Using modern service mapping principles, we can convert raw asset data continuously into meaningful operational data whereby it is metadata- and tag-driven, cloud- and container-aware, and aligned to CSDM service definitions. This enables:

- Accurate blast radius analysis
- Business-aware incident prioritization
- Reliable change impact assessment
- Faster and more precise root cause analysis

Multi-Tool Environment—A Reality

Technological development has been an evolutionary journey with organizations embracing the best-of-breed software systems, applications and databases at each phase of this journey to run their business. Today, AI and agentic AI technologies are fueling discovery, monitoring, observability and operations.

Modern enterprises rarely operate on a single IT operations platform. Instead, they run 15-20+ specialized tools across monitoring, cloud, security, DevOps, and ITSM domains. Our observation is that:

Large enterprises average 5–15 monitoring/ observability tools

70%+ **of incidents require data from multiple tools**

>50% **of MTTR is spent on correlation and triage, not resolution**

When organizations accumulate IT tools that are similar in purpose, it leads to increase in:

Duplicate alerts

Fragmented ownership

Inconsistent service views

Higher operational cost

This is the reason why businesses need to have architectural separation of responsibilities, where tools specialize but integrate through a common operational data backbone.

In fact, leading service providers and enterprise architects are converging on a 3-system operating model (discussed below). To ensure consistency in the process of detection, decision and action throughout ITOM, many service providers (for example, ServiceNow) are adopting separation of concerns design principle to increase modularity, maintainability, and scalability of software systems. The separation is expressed in terms of:

System of detection for generating telemetry and signals.

System of record for normalizing, contextualizing and governing.

System of action for executing workflows and taking remedial actions.

Let us discuss each of these separations in more detail.

System of detection for generating telemetry and signals

The purpose of this system is to generate raw signals about system behavior.

Its typical capabilities include, and not limited to:

- **Metrics collection**
- **Logs**
- **Events/alerts**
- **Traces**

- **Synthetic monitoring**
- **APM**
- **Infrastructure discovery**

Generally, these tools are categorized as:

- **Observability platforms**
- **Application Performance Monitoring (APM) solutions**
- **Network monitoring**

- **Cloud-native monitors**
- **Security signals**
- **Discovery scanners**

The key characteristics of this system are as follows:

- **High volume (millions of events/day)**
- **Short retention**

- **No business context**
- **Technology-centric**

Without the integration of the above, businesses would face challenges such as signal noise, duplicate alerts, siloed dashboards, and absence of service impact visibility, to mention a few.

System of record for normalizing, contextualizing and governing

The purpose of this system is to convert signals into business-relevant, governed knowledge. This is where the CMDB/Service Graph operates.

A system of record helps to:

- **Normalize incoming data**
- **Deduplicate entities**
- **Reconcile identities**
- **Enrich with ownership & cost**

- **Map dependencies**
- **Provide service context**
- **Govern lifecycle & compliance**

This layer is critical because it enables organization to address aspects such as:

- **Multiple versions of the truth**
- **Inconsistent naming**
- **Orphan assets**

- **Incorrect impact analysis**
- **Poor change risk assessment**

The ServiceNow CMDB functions as an authoritative model—

a knowledge graph connecting business → services → applications → infrastructure → people → risk → cost.

It enables outcomes such as:

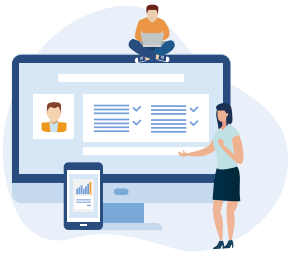
- **Root cause isolation**
- **Change risk scoring**
- **Service health**

- **Compliance reporting**
- **FinOps alignment**

System of action for executing workflows and taking remedial actions

The purpose of this system is to turn insights into automated remediation. Its capabilities include, and not limited to:

- **Incident creation**
- **Workflow orchestration**
- **Runbooks**
- **Auto-remediation**



- **Change automation**
- **Provisioning**
- **Ticketing**
- **Notifications**

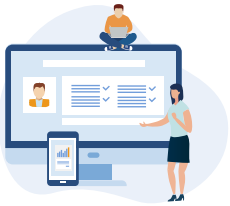
The main characteristics of this system are as follows:

- **Policy-driven**
- **Workflow-based**

- **Human + automation hybrid**
- **Agentic**

The benefits of a system of actions are many and we highlight a few key ones:

- **Reduced MTTR**
- **Consistent processes**



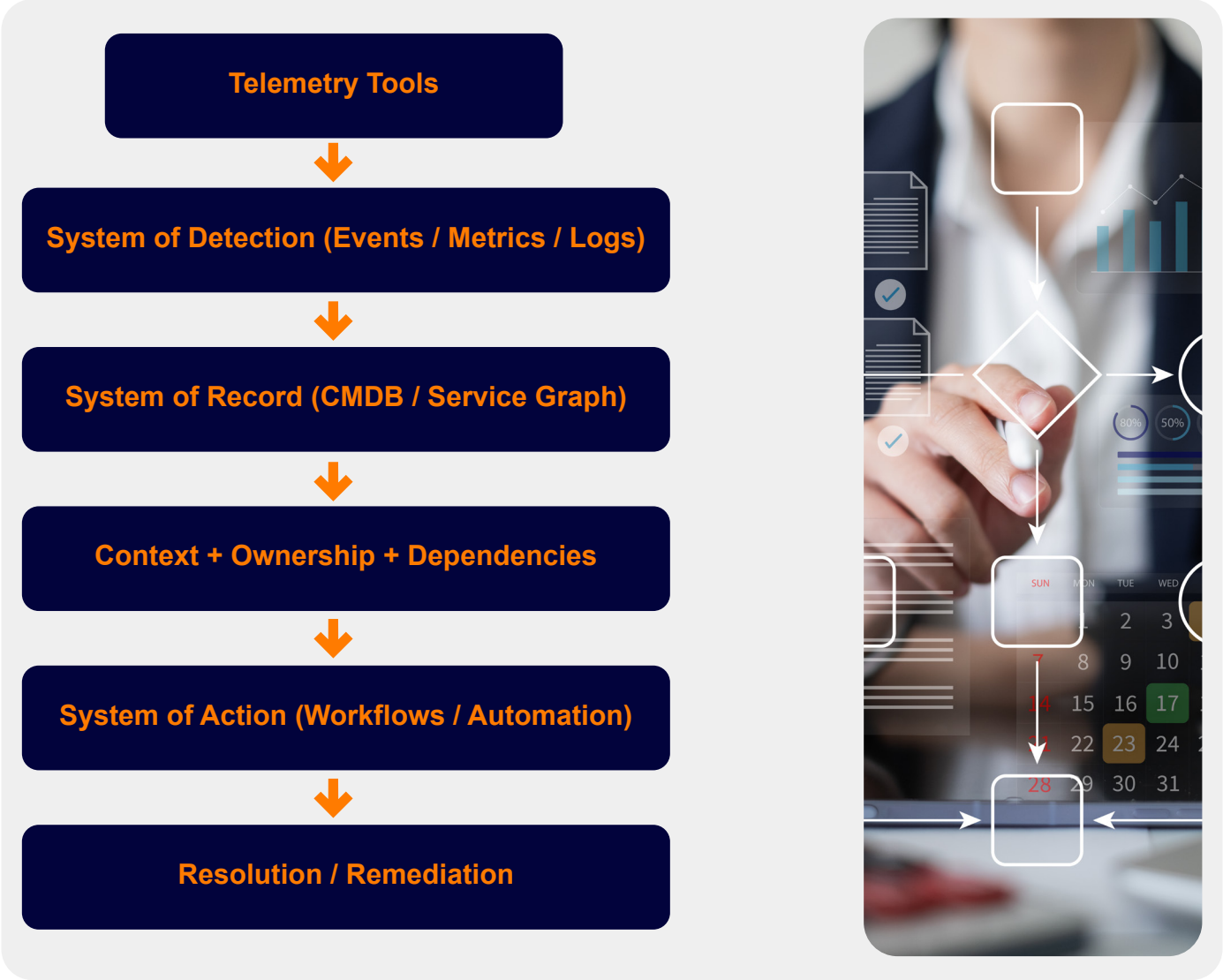
- **Fewer manual steps**
- **Closed-loop operations**

As organizations increase the number of IT tools across their business, the more important it becomes to have a strategy that can integrate these systems into the ServiceNow ecosystem through, for example:

- **Event ingestion into event management**
- **Service graph connectors**
- **API-based telemetry integration**

- **MID Server integrations for on-prem systems**
- **Reconciliation into CMDB as the authoritative model**

This approach avoids shadow systems and ensures consistent reasoning across tools. If you were to imagine the flow of an Integrated Operating Model (of Detection → Record → Action), it would resemble this flow:



This pattern creates: Signal → Insight → Action
Data → Knowledge → Outcome

Modern IT operations require a layered architecture where detection systems generate signals, a centralized system of record contextualizes and governs enterprise configuration knowledge, and systems of action automate remediation. This separation of concerns enables scalability, reduces operational complexity, and ensures consistent decision-making across heterogeneous toolchains.

Workflow as the Execution Engine for AI and Agents

AI without workflow remains advisory and agents without workflow remain unsafe.
The ServiceNow platform fulfills both of these requirements. Through its workflow engine, ServiceNow:

- **Enforces the enterprise IT policy**
- **Governs the human-in-the-loop principle**
- **Ensures auditability and traceability**
- **Controls the execution of autonomous actions**

In an agentic architecture, the CMDB knowledge graph enables reasoning, derives insights and governs workflow execution.

Graph-based and visual representations of operational data are critical for human operators, AI systems and autonomous agents.

Acknowledging the significance of this, the ServiceNow platform enables:

Service-centric health and dependency views.

Visual blast radius analysis.

Timeline-based correlation of events, changes, and incidents.

Shared situational awareness across IT and business teams.

Together, these representations operationalize the digital mirror of an organization's infrastructure.

Insights-based Offerings from Nowvia

Our perspective and offerings are grounded in implementation experience across industries and complex enterprise environments. It points to the fact that:

- AI and agentic operations **succeed or fail** based on architecture and data foundations, not algorithms alone.
- CMDB must be treated as a **living knowledge graph,** not a static repository.
- Workflow is the **critical control plane** for agentic execution.

We support organizations in their transformation journeys, specifically through:

- CMDB and service graph maturity assessments
- ITOM architecture and tool rationalization workshops
- Enterprise service mapping programs
- Event management and AIOps implementation
- Automated remediation and runbook orchestration
- AI-enabled service operations using Now Assist

For businesses looking to strengthen their **foundational readiness for AI and agentic operations, we support the following initiatives:**

CMDB hydration and governance aligned to CSDM

Enterprise-scale service mapping and dependency modeling

Multi-source telemetry ingestion using Service Graph Connectors and MID servers

ITOM Center of Excellence design and operating models with a focus on:

- CMDB governance and data quality management
- Discovery and service mapping standards
- Integration strategy across observability tools
- Automation and remediation frameworks
- Operational data standards aligned with CSDM
- AIOps model governance and tuning

For businesses looking to **conceptualize and implement agentic execution across service operations,** we deliver **NowVia Agent Value Packs**—production-grade, domain-aware agentic workflows built natively on ServiceNow and Now Assist. These are deployed across:

- Incident and Major Incident Management
- Change and Release
- Problem Management
- Service Health, Observability, and Remediation

Each solution is designed for safe, explainable, workflow-governed automation at scale.

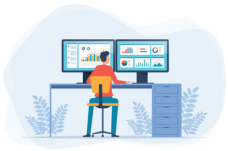
While this paper focuses on ITOM, NowVia also applies **agentic patterns across business workflows** such as HR, Procurement, Third-Party Risk Management (TPRM) and Financial Services Office (FSO), extending AI-driven outcomes beyond IT.

We do not stop at preparing CMDB for AI. We help clients operationalize agentic solutions end-to-end—translating architecture into action. We help enterprises gain the ability to:

Prevent incidents through predictive insights.

Accelerate triage and root cause analysis.

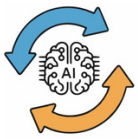
Quantify and mitigate change risk.



Execute automated remediation and self-healing.

Prioritize work based on business impact.

Continuously improve through closed-loop learning.



This integrated surface is also what makes agentic AI safe and effective. AI agents require trusted context, governed data, and controlled execution boundaries. **Without an authoritative service model, automation amplifies risk. With it, automation amplifies resilience.**

Operational Excellence as an Architectural Choice

The next phase of IT Operations Management will not be won by adding more tools. It will be won by architecting clarity, context, and control into the enterprise fabric.

Over the past decade, enterprises have accumulated a rich ecosystem of monitoring, observability, cloud, and automation platforms. While each delivers specialized value, tool sprawl has unintentionally increased operational noise, fragmented ownership, and slowed decision-making. The combined impact of this is often reflected in increased cost, longer time to market, poor customer service and inadequate compliance with various regulations. The limiting factor is no longer technology capability—it is structural coherence.

As discussed earlier in this paper, operational excellence emerges when organizations deliberately separate concerns and align their operating model around a system of detection, record and action. And when CMDB—implemented as a knowledge graph and structured through the Common Service Data Model—serves as the enterprise's operational backbone, connecting business services, applications, infrastructure, ownership, risk, and cost, what you get is a single view that you can trust,

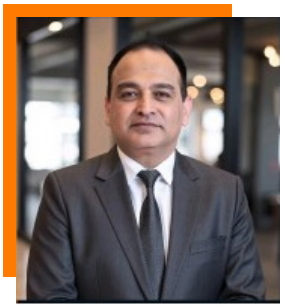
Platforms such as ServiceNow demonstrate how its architectural foundation enables service mapping, AIOps, and workflow orchestration to operate cohesively rather than independently. When these capabilities converge, operations evolve from reactive firefighting to intelligent, preventative service management.

The future of ITOM is not incremental optimization—it is architectural intent. Organizations that treat operational excellence as a structural design choice—rather than a collection of tools—will achieve:

In the age of AI and autonomous operations, the differentiator is clear: **Operational excellence is not something organizations buy. It is something they architect.**

Authors

Manisha Sriraman
Chief Technology Officer



Syed Rizvi
Vice President - Presales & Solution

Contributors

Ravi Gaurav
Senior Solution Architect

About NowVia

NowVia is a **ServiceNow-first digital transformation partner.** We work closely with businesses across industries to maximize and unlock hidden business value by stabilizing, expanding, and modernizing their ServiceNow ecosystems. We specialize in advanced, intelligent workflow design, agentic architecture, and system integration, enabling organizations to fully leverage ServiceNow as their enterprise orchestration hub.

Visit us at https://www.nowvia.com/

Disclaimer

This document is intended for general informational purposes only and to service as advisory.

Endnotes

[1] Gartner Survey Finds 54% of Infrastructure & Operations Leaders Are Adopting AI to Cut Costs. The overall spending on IT operations management software has continued to grow and is expected to reach $81 billion by 2028. How much of this will be geared to AI-based operation management remains to be seen. For details, see Forecast: IT Operations Management Software, Worldwide, 2022-2028, 2Q24 Update.

[2] According to research conducted by Accenture, AI-augmented workflows led to a growth rate that was 4.7 times faster for top performing AI adopters and the company's own sales team increased productivity by 35%. For complete details, see Rethinking IT operating models. For how and why CIOs can play a key role in shaping their ITOM to support the overall executive expectations and value or outcomes of technology investments, see Gartner Research titled: How CIOs Deliver and Show Value From the IT Operating Model.

[3] For a good analysis of why and how graphs are reshaping IT management, see The Graphic Future Of IT Management.

[4] For an interesting perspective on this aspect, see Unlock IT Operational Excellence In Seven Steps (Part 2) and Revolutionizing IT Operations Comes With Manageable Risks (Part 3).

[5] AI ROI: The Paradox of Rising Investment and Elusive Returns.

[6] Ibid. See also: AIOps Is Booming — So Why Isn't The Payback Obvious?

[7] In its 2024 Market Share Report, Gartner placed ServiceNow in #1 position in six tech workflow segments. For details see ServiceNow ranks No. 1 in 6 tech workflow segments.

[8] For more details, see Large Financial Institution Streamlines Incident Management using AIOps from Moogsoft

[9] For further details, see How can a new CMDB deliver great healthcare?

[10] See, for instance, Audit Nightmares: The Challenges of Facing IT Audits with an Inaccurate CMDB ; Outdated Tech, Rising Risk: How Federal Agencies Can Eliminate Tech Debt and Reduce Cyber Risk ; Global manufacturing organization modernizes ITAM strategy with ServiceNow. Remember the cyber breach exposing ~5.8 million customer records at Bayview, a large mortgage lender? Bayview Asset Management Data Breach and $20M Settlement – CISO Analysis ;

[11] For details, see Unifying IT and Non-IT Asset Visibility for 100+ Branches at a Leading Indian Bank Using ServiceNow for Banking

[12] Intelligence in, intelligence out: How Dynatrace and ServiceNow are powering autonomous IT . For an example from the healthcare industry where the healthcare provider's AI ops tools reduced noise and improved MTTR, validating that a reasoning framework (accurate data + governance) and ensuring safe, scalable automation, see Healthcare: Context-Infused CMDB Data & Automated Workflows Bolster ServiceNow Investment.