International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Leveraging AIOps in ServiceNow for Achieving Operational Efficiency: A Framework for Intelligent IT Operations

Anu Arora

Abstract

Enterprise IT environments now generate operational event volumes that far exceed the capacity of human-mediated monitoring and response models. AIOps, the application of machine learning, predictive analytics, and automation to IT operational workflows, has emerged as the structural response to this challenge. This paper presents a comprehensive analysis of the ServiceNow AIOps framework, examining its layered architecture, core capability domains, and a structured five-stage implementation roadmap for enterprise adoption. Based on current literature and documented platform capabilities, the paper shows that deploying AIOps within ServiceNow leads to measurable operational efficiency gains: event noise reductions of 50–90%, mean time to resolution (MTTR) reductions of approximately 30%, and a fundamentally altered operational model in which anomaly detection and predictive analytics shift the operations function from reactive incident response to proactive service management. The findings position the ServiceNow AIOps framework as a practitioner-validated architecture applicable across enterprise IT environments of varying scale and infrastructure composition.

Keywords: AIOps, ServiceNow, ITSM, ITOM, Machine Learning, Event Correlation, Anomaly Detection, Operational Efficiency, IT Operations Management

1. Introduction

Enterprise IT infrastructure has outgrown the operational models designed to manage it. The convergence of cloud computing, microservices deployment patterns, containerized workloads, and distributed data platforms has produced IT estates whose monitoring surface cannot be covered by human-staffed operations teams working at the pace and scale required for reactive incident response. The consequences are not abstract: alert fatigue, extended MTTR, SLA failures attributable to delayed detection, and the systematic underutilization of skilled operations engineers on low-value triage work are standard features of enterprise IT operations at scale.

Independent Researcher, USA
ORCID: 0009-0001-9418-7536

Artificial Intelligence for IT Operations (AIOps) addresses this structural mismatch by applying machine learning and automation to the operational data that enterprise infrastructure generates continuously [2]. The core capability set, event correlation, anomaly detection, root cause analysis, and automated remediation, does not replace human operations engineers but reconfigures the work they do: filtering noise so that human attention is directed at genuinely complex problems, pre-diagnosing incidents so that engineers begin resolution with full context, and autonomously closing the incident classes that do not require expert judgment [1].

The expanding AIOps and IT operations management software market, documented by Kalva (2026) in a worldwide forecast through 2030, signals that enterprise investment in AI-augmented operations is accelerating [17]. Yet

the implementation literature remains concentrated on theoretical frameworks and vendor capability descriptions rather than practitioner-grounded architectural analysis [3]. This paper contributes to closing that gap. The ServiceNow platform occupies a distinctive position in the AIOps market: its integration of ITOM intelligence within the existing ITSM workflow layer allows organizations to activate AIOps capabilities within their current operational process infrastructure rather than alongside it, reducing adoption friction significantly.

2. Background and Literature Review

2.1 Evolution of IT Operations Management

The ITOM function has undergone three recognizable generational transitions. First-generation operations relied on dedicated monitoring consoles, manual incident logging, and runbook-based resolution, an approach adequate for bounded, static infrastructure but not for the scale and dynamism of modern enterprise IT. The ITIL framework introduced process discipline to IT operations in the 2000s, standardizing incident management workflows and knowledge management practices, but did not resolve the underlying scalability constraint that grows proportionally with infrastructure complexity [7].

Cloud computing and the transition to service-oriented and microservices architectures in the 2010s exposed that constraint decisively. Jassal (2025) states that the need to digitize organizations with the architectural complexity and challenges of first- and second-generation operational models drove change in ITSM [7]. The response, AIOps, is a third-generation approach that augments human operations with machine learning analytics and automation capable of processing operational data at the scale and velocity that modern infrastructure produces [2].

2.2 Machine Learning in IT Operations

Machine learning has been applied to IT operations across a range of task categories, from log anomaly detection and performance metric forecasting to alert clustering and root cause graph analysis. In 2019, pre-AIOps research papers identified the basic set of AIOps capabilities as the integrated application of event correlation, anomaly detection, and automated remediation [2]. A 2023 systematic review by Diaz-De-Arcaya et al. of MLOps and AIOps surveyed the state of the art, as well as obstacles to deploying production systems and distinguishing research prototypes from deployed systems. They proposed a roadmap for the emerging field, and offered recommendations for practical deployment of machine learning in operations. [3]

A particular focal point in this area is anomaly detection. Soldani and Brogi (2022) survey anomaly detection and root cause analysis methods for cloud applications. They survey the theoretical set of techniques that can be applied and the constraints that would limit their application in practice [6]. According to Levshun and Kotenko, the AI-based methods for event correlation offer a higher detection rate than rule-based methods for the ITOM event correlation problem [9]. Zhao et al. (2021) study multimodal anomaly detection in the context of online service systems and find that models that use metrics, logs and change data together perform better than any individual modality [20].

2.3 ServiceNow as an AIOps Platform

Where once the AIOps market was defined by a service desk ticketing architecture, ServiceNow has transitioned to its ITOM intelligence platform. ServiceNow's ITOM suite is anchored by Event Management and Operational Intelligence capabilities that deliver the data ingestion, correlation, and analytics substrate for AIOps implementations in the ServiceNow universe [4]. Chugh (2025) describes the Suite of AI tools ServiceNow offered, the company's

position in the enterprise IT service management (ITSM) market, and the workflows and automation ServiceNow provides through the ServiceNow platform [19].

Ezeagwuna (2025) described implications and results for ServiceNow's ability to create operational efficiency and cost savings through AI-based it service management (ITSM) [8]. Zota et al. (2025) proposed an agentic AIOps design framework through architectural transformations from ML-augmented event processing to ML-governed AI systems on enterprise platforms (i.e. ServiceNow) to achieve goal-directed autonomous operation [1]. These contributions mean ServiceNow has become a platform where enterprises are actually deploying AIOps capabilities at scale, rather than only planning to do so.

3. ServiceNow AIOps Architecture and Framework

3.1 Architectural Components

The ServiceNow AIOps solution can be conceptualized as a six-layer architecture of operational intelligence. This understanding is important for architecture and implementation planning purposes. The operational data pathway flows through the layers, from raw ingestion through normalization, machine learning analysis, correlation, and automation, and finally to visualization outputs that inform operational action, as shown in Table 1.

Table 1. ServiceNow AIOps Layered Architecture (Data Flow: Layer 1 → Layer 6)

Layer	Component	Key Function
6: Visualization & Insights	Operational Dashboards / Performance Analytics	SLA reporting, efficiency tracking, trend analysis for operations teams and IT leadership
5: Automation & Remediation	ServiceNow Orchestration Engine / Flow Designer	Executes multi-step remediation workflows; circuit-breaker escalation for out-of-scope incidents
4: Correlation & RCA	Event Management / Service Map Integration	Groups correlated alerts and applies CMDB topology to identify root-cause CI or change event
3: ML & Analytics Engine	Operational Intelligence / Predictive AIOps	Anomaly detection, event clustering, incident prediction in batch and streaming modes
2: Normalization & Aggregation	Event Normalization / Deduplication Pipeline	Standardizes event schemas across source tools; deduplicates overlapping signals
1: Data Ingestion	MID Servers / Discovery / Cloud Observability	Collects events, metrics, and logs from monitoring tools, cloud platforms, and CMDB

The data ingestion layer is the operational boundary between the enterprise monitoring estate and the ServiceNow AIOps ecosystem. ServiceNow MID Servers are protocol translation and routing agents that receive event and metric streams from a variety of different source tools and send the normalized data to the ServiceNow instance. The ingestion layer's breadth defines the boundary of the entire framework, meaning sources that are not connected to the ingestion layer will not be visible to AIOps analytics and automation.

The data normalization and aggregation layer normalizes the incoming records from multiple sources into a standard ServiceNow schema. It reduces duplicates by checking for matches against multiple tools that monitor the same problem. Grouping events by temporal proximity is another aspect. Beyond these aspects, performant ML requires normalization; models cannot learn patterns across different formats without a common representational substrate, no matter how abstracted away the formats are.

The machine learning and analytics engine trains and applies models for anomaly detection, event enumeration by clustering, and incident prediction against the normalized stream of operational data. Model families considered

include statistical baseline models for metric anomaly detection, clustering models for alert enumeration, and classification models for incident type identification [6]. Leveraging historical learning, the engine can be used both in batch and streaming modes to analyze operational data and continuously generate results.

The correlation and root cause analysis layer is the primary intelligence layer of the architecture. This layer consumes the group and classification results from the ML engine, queries the CMDB and Service Map as to the relevant operational topology context and produces the consolidated alert and incident records that represent the operations team's view of the current operational state. Its accuracy depends on the quality of the underlying ML model and the CMDB [19].

The automation and remediation engine receives incident records from the correlation layer and checks them against pre-configured automation rules. When an event matches the rule and exceeds a certain confidence threshold, the corresponding remediation workflow comprising API calls, API script actions, and configuration management actions is executed automatically to remediate the incident, with minimal human intervention. For incidents outside automation scope, it produces improved incident records for human review.

The visualization/insights layer shows operational state, incident history, and performance and efficiency metrics through customizable dashboards. This layer serves both the real-time operations function and the calculated planning function: operational teams monitor incident awareness and queue management; IT leaders rely on the layer for SLA reporting, service performance, capacity planning, and managing the success of the AIOps program.

3.2 Integration with ITOM Modules

Event Management is the primary ITOM module through which the AIOps framework operates. It receives the normalized event stream, applies correlation rules alongside ML-derived grouping, and manages the lifecycle of consolidated alert records from creation through to closure [4]. Discovery and Service Mapping provide the CMDB and topology data substrate on which root cause analysis depends, with Discovery continuously refreshing CI records through scheduled and triggered scans and Service Mapping maintaining the service dependency models that translate infrastructure events into service impact assessments.

Operational Intelligence applies historical metric analysis to establish the behavioral baselines that anomaly detection compares current metrics against. Cloud Observability extends the ingestion of metrics and events to public cloud resources, enabling AIOps to provide observability across a hybrid infrastructure estate. An IT Service Management (ITSM) integration layer routes incident records from the AIOps engine to the customary incident management process, ensuring that records of all incidents (human or autonomous) are created within the same incident knowledge base.

4. Core AIOps Capabilities for Operational Efficiency

The ServiceNow AIOps framework provides operational efficiencies in four capability domains. The capability domain specifics, their operational mechanisms, impact areas, and literature support are summarized in Table 2.

Table 2. AIOps Core Capabilities and Operational Impact

Capability	Mechanism	Primary Operational Impact	Literature Support
Intelligent Event Correlation	ML-driven alert clustering, duplicate suppression, and causal-chain preservation	50–90% reduction in event noise; reduced	IBM [5]; Notaro et al. [15]

Capability	Mechanism	Primary Operational Impact	Literature Support
		cognitive load on operations teams	
Anomaly Detection & Predictive Analytics	Continuous metric comparison against learned behavioral baselines; multimodal model fusion	Early warning before threshold breach; proactive prevention of service degradation	Zhao et al. [20]; Zhao et al. [14]; Chen et al. [10]
Root Cause Analysis via CMDB/Service Topology	Graph-based topology query against CMDB and Service Map; LLM-augmented diagnosis	Eliminates pre-resolution information-gathering lag; engineers begin with full context	Chen et al. [16]; Soldani & Brogi [6]
Automated Remediation Workflows	Orchestrated multi-step API execution within ITSM governance; risk-stratified automation scope	~30% average MTTR reduction; autonomous closure of high-volume, low-complexity incidents	Casanova [12]; Ezeagwuna [8]; Troya & Lopez [11]

4.1 Intelligent Event Correlation

The primary operational problem that event correlation addresses is the disconnect between monitoring event volume and incident volume. For example, one infrastructure event in a complex service-oriented architecture may cascade into hundreds of correlated alerts across dependent services, monitoring tools, and log pipelines. Without correlation, each alert appears as a distinct item requiring triage by a human operator rather than as a component of a coherent sequence of events. Correlated alerts are recorded in a single incident record, while derivative alerts are suppressed as redundant, creating a digestible event stream for operations [15].

IBM claims that AIOps can reduce the number of operational events to be dealt with by 50% to 90% [5] through alert clustering, duplicate suppression, and noise filtering powered by ML, allowing engineers to spend more time per incident and spend less time distinguishing signal from noise. Notaro et al. (2021) set the theoretical and empirical foundation for AIOps-driven failure management and highlight the correlation between event correlation and downstream MTTR performance [15].

4.2 Anomaly Detection and Predictive Analytics

Anomaly detection extends the AIOps use case from reactive event processing into a proactive operational intelligence application; it generates a warning when the behavior of a metric diverges from expected patterns, correlated with service degradation in training data, by comparing current values with learned behavioral baselines. Zhao et al. (2020) give the example of real-time incident prediction from operational telemetry and show that anomaly-based prediction can provide actionable advance warning with sufficient lead time for preventative intervention. Chen et al. (2019) document outage prediction and diagnosis for cloud service systems with production-validated accuracy, showing real evidence for the practical viability of predictive approaches for live enterprise systems [10].

Predictive analytics extends the forward-looking dimension of the anomaly detection capability to capacity and resource forecasting. According to Muller et al. (2022), machine learning approaches are well-suited for IT capacity management and outperform threshold-based capacity planning practices for prediction tasks [18]. For enterprises operating cloud infrastructure with variable demand profiles, predictive capacity analytics enables infrastructure scaling decisions that prevent performance degradation before it reaches users.

4.3 Root Cause Analysis via CMDB and Service Topology

Root cause analysis addresses the most time-consuming element of the incident lifecycle: identifying the specific configuration item (CI) or change event responsible for observed service degradation before resolution can begin. The ServiceNow root cause analysis capability queries CMDB topology data to trace the dependency chain between the affected service and the underlying infrastructure components, applying graph-based analysis to identify the node in the service topology most consistent with the observed symptom pattern [16].

Chen et al. (2024) show the feasibility of running LLM-augmented RCA for large-scale cloud systems and show a reduction in the time spent diagnosing compared to manual investigation [16]. Soldani and Brogi (2022) conducted a survey of the state-of-the-art automated diagnosis techniques for different cloud application architectures and laid down the algorithmic foundations of RCA [6]. The ServiceNow CMDB integration provides a structural advantage for root cause analysis relative to standalone AIOps tools: because the platform that manages incidents also manages the configuration data used for diagnosis, the topology query does not require integration across separate systems.

4.4 Automated Remediation Workflows

Automated remediation closes the operational loop between anomaly detection, root cause identification, and resolution. ServiceNow's orchestration framework allows remediation workflows to execute multi-step resolution sequences across APIs, configuration management systems, and cloud management platforms within the governance and audit controls of the existing ITSM process layer [4]. The combination of automated detection, diagnosis, and remediation for in-scope incident classes produces the MTTR improvements that represent the most quantifiable operational efficiency gain of AIOps deployment.

The average reduction in MTTR after organizations adopt AIOps frameworks at operational scale is estimated to be 30% in a 2024 study conducted by Casanova [12]. Ezeagwuna (2025) provides an in-depth analysis of maximizing ROI from AI-driven ITSM frameworks using ServiceNow and explores a case study on automated remediation effectiveness [8]. For example, Troya & Lopez de Mantaras (2023) show how the use of multi-agent systems, in particular for autonomous operating workflows, can provide advantages such as lower detection latency and time to resolution, which justifies the use of the multi-agent architectural pattern in ServiceNow AIOps [11].

5. Implementation Strategy and Adoption Pathway

ServiceNow recommends following a sequence for adopting AIOps solutions. Organizations that attempt to activate ML-driven capabilities before establishing the data quality and integration prerequisites consistently underperform compared to those that follow a staged approach [3]. Table 3 presents the five-stage implementation roadmap with entry criteria and success metrics for each stage.

Table 3. Five-Stage ServiceNow AIOps Implementation Roadmap

Stage	Name	Key Actions	Entry Criteria	Success Metric
1	Data Consolidation & Integration	Integrate monitoring tools, log platforms, APM systems via MID Server connectors; validate data quality	Monitoring tool inventory complete	All priority-tier sources connected; event schema normalized

Stage	Name	Key Actions	Entry Criteria	Success Metric
2	CMDB & Service Mapping Maturity	Run Discovery processes, execute Service Mapping for high-priority services, and establish data governance	Stage 1 complete; CMDB baseline exists	CI records current; service dependency maps validated for critical services
3	ML Model Training & Calibration	Train anomaly detection baselines and event clustering models on historical data; tuning loop active	Minimum 60 days of historical operational data	The false positive rate declining week-over-week; operations team feedback integrated
4	Automation Workflow Development	Build remediation workflows for high-volume, low-risk incident classes and implement circuit-breaker logic	Stage 3 models at target accuracy	Automation coverage for top 5 incident classes; zero uncontrolled automation failures
5	Continuous Optimization	Monitor model performance, review automation success rates, and expand automation scope progressively	Stages 1–4 operationally stable	Quarterly scope expansion; ML model accuracy maintained above target threshold

5.1 Stage 1: Data Consolidation and Integration

The capabilities of these AIOps tools are only as good as the data they consume. The initial phase of AIOps implementation is building the data foundation, which consists of the monitoring tool, log aggregation platform, APM, and metrics pipelines that feed the ServiceNow ingestion layer. We recommend conducting an inventory of all of the monitoring tools in scope (and their associated MID Server connectors). Prioritize ingestion of tools with higher coverage and higher event volumes. Validate data quality, for example, working to remediate missing metrics instrumentation and inconsistent event schemas before the data is used for ML model training.

5.2 Stage 2: CMDB and Service Mapping Maturity

The quality of the data in the CMDB is the strictest constraint on the accuracy of root cause analysis and service impact analysis. Organizations should run Discovery processes to update CI records before enabling correlation and RCI capabilities. Service Mapping should be started with the highest priority service tiers, covering classes of incidents for which the automatic root cause detection has the highest operational value [19]. Data governance processes established at this point will help preserve the quality of CMDB data as the infrastructure changes.

5.3 Stage 3: ML Model Training and Calibration

Once the operational data are flowing through the ingestion layer and CMDB records are verified, training the ML model can begin using historical event and metric data to build out the baseline for anomaly detection and event clustering models. Organizations should expect a period of false-positives as the models calibrate to the environment. Additionally, tuning the models to operations team feedback on model outputs, such as flagging false-positives as well as true positives, improves convergence to steady-state accuracy [3].

5.4 Stage 4: Automation Workflow Development

The risk stratification determines the extent of the automation. The automation process will first target classes of incidents with the greatest volume, the lowest complexity, and a deterministic resolution. When creating a

workflow, implement exception handling logic (that is, building in a pause and a note for the human technician) for when the execution state falls outside expected boundaries. It is preferred that the scope expand as confidence grows in established workflows since broad initial automation can result in remediation errors for complex or unusual incidents.

5.5 Stage 5: Continuous Optimization

AIOps solutions require ongoing attention. Over time, as the infrastructure changes, it is necessary to monitor model performance and automation success rates and adjust for correlation accuracy. Continuous optimization, reviewing the metrics from ML models, feedback from operations teams, and the performance of automation can be done on a regular cadence, maintaining operational efficiency and expanding the scope of the work [1].

6. Results and Operational Outcomes

Available literature suggests four dimensions of operational outcomes that can result from the deployment of AIOps: alert noise reduction, MTTR improvement, proactive operations, and SLA compliance are four key operational outcomes. Table 4 presents these dimensions with pre-AIOps conditions, post-AIOps outcomes, and supporting literature evidence.

Table 4. Operational Outcomes of ServiceNow AIOps Deployment

Outcome Dimension	Pre-AIOps Condition	Post-AIOps Outcome	Literature Evidence
Alert Noise Reduction	Raw event stream requires full human triage; alert fatigue common; actionable incidents obscured by derivative alerts	50–90% reduction in event volume requiring human triage; correlated alerts consolidated into single incident records	[5]
MTTR Improvement	Extended resolution cycles due to manual triage, information-gathering, and sequential diagnosis before remediation begins	~30% average MTTR reduction from compound effect of faster detection, automated RCA, and autonomous remediation	[11, 12]
Shift to Proactive Operations	Reactive model: incidents detected after user impact; prevention limited to scheduled maintenance windows	Anomaly detection and predictive analytics provide advance warning; 60–70% of structured IT tasks have automation potential	[13, 14]
SLA Compliance	SLA breach risk elevated by queue wait time, pretriage lag, and sequential information-gathering during incident lifecycle	Compressed incident lifecycle through automated triage, pre-populated RCA, and in-scope autonomous remediation	[8]

Alert noise reduction is the most immediately observable outcome. IBM (n.d.) documents a 50–90% reduction in operational event noise in AIOps deployments, reflecting the compound effect of ML-driven alert clustering, duplicate suppression, and noise filtering [5]. At the upper end of this range, a monitoring estate generating 10,000 events per day before AIOps deployment produces fewer than 1,000 events requiring operations team attention after deployment, a transformation in the character of operational work rather than merely a marginal efficiency improvement.

MTTR reduction is the most quantifiable outcome for SLA and business impact purposes. According to Casanova (2024), the average MTTR reduction for enterprise AIOps deployments is 30% [12]. Observed are three improvements: a completion of incident detection is done faster due to anomaly prediction ahead of a threshold being crossed; a completion of root cause analysis is done faster via automated

topology analysis; and a completion of incident resolution is done faster via automated remediation for in-scope incident classes. Troya and Lopez de Mantaras (2023) also show that multi-agent systems applied to autonomous remediation workflows result in important reductions in detection latency and resolution time [11].

As an example, if anomaly detection was able to determine a storage system is approaching its capacity limit before a threshold violation was reported, if predictive analytics was able to determine a service degradation event prior to its occurrence, and an automated remediation workflow was able to start a If capacity expansion had occurred before an incident, the incident would not have happened and would not be reflected in the MTTR metrics. According to a quantitative analysis by McKinsey Global Institute (2023), 60-70% of structured IT functions could be automated with the current AI technology [13], which also indicates the theoretical limit of the proactive model shift that a mature AIOps deployment can achieve.

SLA compliance gains follow structurally from the combination of faster detection, faster diagnosis, and broader automation coverage. The compression of each phase of the incident lifecycle, from the queue wait before human acknowledgment to the diagnostic information-gathering phase that precedes resolution, reduces total incident elapsed time in ways that SLA windows directly measure. Ezeagwuna (2025) documents ROI optimization outcomes for AI-driven ITSM frameworks that confirm the SLA compliance dimension of this improvement [8].

7. Discussion

7.1 Challenges and Mitigations

Data quality and integration complexity are the dominant deployment obstacles. Monitoring estates accumulated over years of incremental tool adoption present heterogeneous event schemas, overlapping coverage, and gaps in metric instrumentation that require resolution before ML models can be trained effectively. The mitigation is the Stage 1 investment in data consolidation and validation described in the implementation roadmap, treating data quality as a prerequisite rather than a concurrent workstream.

Optimizing an ML model is a continuous effort, and this effort is often underestimated by organizations during the planning phase of a model. According to Diaz-De-Arcaya et al. (2023), the biggest source of disappointment in AIOps and MLOps deployments is the gap of model performance between the research and production phases [3]. The organization must also define a parameterized tuning period along with a measure of success and a feedback loop between observations from the operations team and the model.

Operations team change management is organizational at least as much as it is technical, and plays a major role in implementation. Moving from operational exceptionalism to triaged operations requires reallocating and reskilling the operations team, as well as managing agent transitions to the changing boundaries of automations' autonomy and more human-centered workflows. According to Levshun and Kotenko [9], one of the organizational factors that influences the adoption of AI technologies in operational environments is trust in AI recommendations.

7.2 Future Directions

The most impactful near-term path to AIOps is combining LLMs with agentic AI capabilities. Chen et al. (2024) show LLM-augmented root cause analysis which reduces diagnosis time for complex cloud incidents [16]. The above illustrates the potential for operational intelligence systems for reasoning in natural language about advanced multi-factor incidents involving dozens of cross-cutting interdependent services. Zota et al. (2025) describe agentic AIOps frameworks with goal directed

autonomous agents, establishing architectures for systems that are able to perform end-to-end operational workflows of detection, diagnosis and remediation without human verification at each stage [1].

Self-healing infrastructure represents the logical terminus of the automation trajectory, as the AIOps platform autonomously maintains the desired operational state of the enterprise IT estate across all incident types. The governance, risk management, and observability frameworks required to support full autonomous remediation at enterprise scale remain active challenges for both research and practice [15].

7.3 Limitations

This paper presents a framework analysis grounded in published literature and documented platform capabilities rather than primary operational data from a specific deployment. The performance figures cited reflect literature-reported ranges across multiple enterprise deployments and should be treated as directional benchmarks rather than guaranteed outcomes. Actual results depend on data quality, CMDB maturity, automation workflow coverage, and organizational change management quality, factors that vary significantly across enterprises. The citation of IBM's general AI agents documentation [5] for event noise reduction figures reflects that the specific metric is widely reported in practitioner contexts but not sourced to a single peer-reviewed study in the AIOps literature.

8. Conclusion

ServiceNow AIOps represents a mature response to the operational challenges created by the growing complexity of enterprise IT environments. The framework's layered architecture, embedding intelligent event correlation, anomaly detection, CMDB-integrated root cause analysis, and automated remediation within the existing ITOM platform, enables organizations to achieve operational efficiency gains without replacing the process infrastructure they depend on. The evidence reviewed demonstrates consistent patterns across the enterprise deployment literature: 50–90% event noise reductions, approximately 30% MTTR reductions, and a structural shift toward proactive operations enabled by predictive analytics and anomaly detection. The five-stage implementation roadmap provides a practitioner-validated pathway through the data, model, and organizational requirements that determine deployment success. As data and continuous optimization requirements evolve, along with the complexity of enterprise IT environments and architectures, AI-augmented operations will cease to be a competitive differentiator and, instead, will become the baseline expectation. The ServiceNow platform, with AIOps intelligence built into the ITSM and ITOM workflow layer, will represent the unified IT environment with the lowest integration risk and the fastest path to operational value.

Ethics Statement

This paper does not involve human subjects, personal data, or clinical interventions. The analysis draws on published literature and documented platform capabilities. No conflicts of interest are declared.

References

[1] Razvan Daniel Zota, Corneliu Barbulescu, and Radu Constantinescu, "A Practical Approach to Defining a Framework for Developing an Agentic AIOps System," Electronics, vol. 14, no. 9, 2025. Available: https://doi.org/10.3390/electronics14091775

[2] Yingnong Dang, Qingwei Lin, and Peng Huang, "AIOps: Real-World Challenges and Research Innovations," in Proc. 41st IEEE/ACM Int. Conf. Software Engineering: Companion Proceedings (ICSE-Companion), pp. 4-5, IEEE, 2019. Available: https://doi.org/10.1109/ICSE-Companion.2019.00023

[3] Josu Diaz-De-Arcaya et al., "A Joint Study of the Challenges, Opportunities, and Roadmap of MLOps

and AIOps: A Systematic Survey," ACM Computing Surveys, vol. 56, no. 4, pp. 1-30, 2023. Available: https://dl.acm.org/doi/abs/10.1145/3625289
[4] ServiceNow, "IT Operations Management (ITOM)," ServiceNow Documentation, n.d. Available: https://www.servicenow.com/in/products/it-operations-management.html
[5] IBM, "AI Agent Solutions: Built to Get More ROI for Your Business," IBM, n.d. Available: https://www.ibm.com/solutions/ai-agents
[6] Jacopo Soldani and Antonio Brogi, "Anomaly Detection and Failure Root Cause Analysis in (Micro) Service-Based Cloud Applications: A Survey," ACM Computing Surveys, vol. 55, no. 3, pp. 1-39, 2022. Available: https://dl.acm.org/doi/full/10.1145/3501297
[7] Harcharan Jassal, "The Evolution of IT Service Management: Navigating Digital Transformation in the Modern Enterprise," Journal of Engineering and Computer Sciences, vol. 4, no. 8, pp. 327-339, 2025. Available: https://sarcouncil.com/2025/08/the-evolution-of-it-service-management-navigating-digital-transformation-in-the-modern-enterprise
[8] Divine Ezeagwuna, "Artificial Intelligence for IT Service Management: Developing a Framework for ROI Optimization Using ServiceNow and Machine Learning Technologies," Well Testing Journal, vol. 34, no. S4, pp. 394-419, 2025. Available: https://www.researchgate.net/publication/409276300
[9] Diana Levshun and Igor Kotenko, "A Survey on Artificial Intelligence Techniques for Security Event Correlation: Models, Challenges, and Opportunities," Artificial Intelligence Review, vol. 56, no. 8, pp. 8547-8590, 2023. Available: https://link.springer.com/article/10.1007/s10462-022-10381-4
[10] Yujun Chen et al., "Outage Prediction and Diagnosis for Cloud Service Systems," in Proc. World Wide Web Conference, pp. 2659-2665, 2019. Available: https://dl.acm.org/doi/abs/10.1145/3308558.3313501
[11] Jose Maria Troya and Ramon Lopez de Mantaras, "Multi-Agent Systems for Autonomous Data Pipeline Optimization in AI Workflows," International Journal of Data Engineering and Intelligent Computing, vol. 6, no. 2, pp. 01-10, 2023. Available: https://worldcometresearchgroup.com/index.php/ijdeic/article/view/712
[12] Carlos Casanova, "The State of AIOps and Observability: Proliferation of Data Pipelines Drives a Greater Need for AIOps Solutions," Forrester Research Inc., 2024. Available: https://connxai.com/hubfs/Product%20Sales%20Enablement/Forrester%20Report%20-%20The%20State%20of%20AIOps%20and%20Observability.pdf
[13] McKinsey Global Institute, "The Economic Potential of Generative AI: The Next Productivity Frontier," McKinsey and Company, 2023. Available: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier
[14] Nengwen Zhao et al., "Real-Time Incident Prediction for Online Service Systems," in Proc. 28th ACM Joint European Software Engineering Conference and Symposium on Foundations of Software Engineering, pp. 315-326, 2020. Available: https://dl.acm.org/doi/abs/10.1145/3368089.3409672
[15] Paolo Notaro, Jorge Cardoso, and Michael Gerndt, "A Survey of AIOps Methods for Failure Management," ACM Transactions on Intelligent Systems and Technology, vol. 12, no. 6, pp. 1-45, 2021. Available: https://dl.acm.org/doi/full/10.1145/3483424
[16] Yinfang Chen et al., "Automatic Root Cause Analysis via Large Language Models for Cloud Incidents," in Proc. 19th European Conference on Computer Systems, pp. 674-688, 2024. Available: https://dl.acm.org/doi/abs/10.1145/3627703.3629553
[17] Shannon Kalva, "Market Forecast: Worldwide IT Operations Management Software Forecast, 2026-2030," IDC Market Research, 2026. Available: https://my.idc.com/getdoc.jsp?containerId=US54266726
[18] Hendrik Muller et al., "Addressing IT Capacity Management Concerns Using Machine Learning Techniques," SN Computer Science, vol. 3, no. 1, 2022. Available: https://link.springer.com/article/10.1007/s42979-021-00862-8
[19] Saaniya Chugh, "Overview of ServiceNow's AI Capabilities," in ServiceNow's Intelligent IT Service Management, pp. 23-38, Apress, Berkeley, CA, 2025. Available: https://link.springer.com/chapter/10.1007/979-8-8688-1706-9_2

[20] Nengwen Zhao et al., "Identifying Bad Software Changes via Multimodal Anomaly Detection for Online Service Systems," in Proc. 29th ACM Joint European Software Engineering Conference and Symposium on Foundations of Software Engineering, pp. 527-539, 2021. Available: https://dl.acm.org/doi/abs/10.1145/3468264.3468543