electronics

Article

A Practical Approach to Defining a Framework for Developing an Agentic AIOps System

Răzvan Daniel Zota [1,*], Corneliu Bărbulescu [2] and Radu Constantinescu [1]

[1] Department of Business Informatics and Cybernetics, Bucharest University of Economic Studies, 010552 Bucharest, Romania; radu.constantinescu@ie.ase.ro
[2] IBM Corporation, 1 Orchard Rd Armonk (HQ), Armonk, NY 10504, USA; corneliu.barbulescu@ro.ibm.com
* Correspondence: zota@ase.ro

Abstract: The increasing complexity of IT operations necessitates advanced automation to ensure system availability, resilience, continuity, performance, security, and maintainability. Traditional IT management frameworks, such as the Information Technology Infrastructure Library (ITIL), have standardized service management processes, while models like IBM's Process Reference Model for IT (PRM-IT) have facilitated automation through structured workflows. However, critical tasks, such as incident resolution and problem management, still require significant human intervention. The adoption of development, security, and operations (DevSecOps) introduced standardized remediation playbooks, further enhancing automation. More recently, Generative AI (GenAI) has expanded automation possibilities, opening new avenues for hyper-automated IT operations. This study explored Agentic Artificial Intelligence for IT Operations (Agentic AIOps), an approach that integrates AI-driven agents to autonomously manage IT operations. Our methodology features a framework for designing and developing an Agentic AIOps system that proactively detects anomalies, classifies incidents, and autonomously executes resolution workflows across infrastructure, middleware, data, and applications in complex, heterogeneous Enterprise IT environments. Our findings suggest that such a system can significantly reduce incident response time, enhance predictive maintenance, and enable self-healing IT environments. By leveraging AI agents for real-time decision making, this approach enhances operational efficiency and reduces human workload. We conclude that this Agentic AIOps system represents a transformative step toward fully autonomous IT operations. We outline a framework for defining its architecture and planning its subsequent development, ensuring continuous evolution and adaptability in complex IT landscapes.

Keywords: AIOps; Agentic AIOps; MLOps; AI-driven agents; ITIL; PRM-IT

check for updates

Academic Editor: Domenico Rosaci

Received: 13 March 2025
Revised: 18 April 2025
Accepted: 25 April 2025
Published: 27 April 2025

Citation: Zota, R.D.; Bărbulescu, C.; Constantinescu, R. A Practical Approach to Defining a Framework for Developing an Agentic AIOps System. *Electronics* **2025**, *14*, 1775. https://doi.org/10.3390/electronics14091775

1. Introduction

The rapid advancement of digital technologies and the increasing complexity of IT infrastructures have transformed the landscape of IT operations. At the same time, emerging IT challenges require enhanced levels of reliability and efficiency in computer systems [1]. To maintain high availability, performance, reliability, efficiency, and security, modern organizations rely heavily on IT Operations Management, which encompasses tasks such as incident detection, problem resolution, and performance optimization. Traditional frameworks such as the Information Technology Infrastructure Library (ITIL) [2] and automation practices such as development, security, and operations (DevSecOps) have standardized workflows and introduced efficiency. Briefly, ITIL is "a library of best practices for managing IT services and improving IT support and service levels" [3]. However, the solutions based solely on traditional frameworks still depend on significant human intervention, particularly for complex problem resolution and decision making. Today, ITIL is a registered trademark currently owned by the United Kingdom's Office of Government Commerce (OGC) [4].

The emergence of Artificial Intelligence for IT Operations (AIOps), first coined by Gartner in 2017, marked a significant step forward [5]. Actually, this concept originally evolved from the earlier concept of IT Operations Analytics (ITOA) [6]. In simple terms, AIOps is "the application of machine learning (ML) and data science to IT operations problems" [7]. Some authors see AIOps as "an emerging interdisciplinary field" [8] at the intersection of research domains such as ML, big data, streaming analytics, and IT operations management. AIOps "has been adopted in organizations in various tasks, including interpreting models to identify indicators of service failures" [9]. Moreover, AIOps systems represent a paradigm shift in IT operations, transitioning from reactive issue handling to proactive, AI-driven operational intelligence. Also, the implementation of AIOps systems can yield substantial benefits, including the assurance of high service quality and customer satisfaction, enhanced engineering productivity, and a reduction in operational expenditures [10]. AIOps systems are particularly valuable for large-scale organizations characterized by heterogeneous application ecosystems, encompassing enterprise systems, monolithic architectures, and microservices, as well as both on-premises and cloud-native environments [11]. For example, when operating in cloud computing environments, AIOps models are capable of efficiently detecting anomalies, identifying root causes, autonomously resolving issues, and managing cloud resources, thereby minimizing the need for manual operational intervention [12].

AI is fundamentally transforming enterprise strategic frameworks and operational models, catalyzing a widespread wave of AI-driven transformation across diverse industries, like the case of enterprise businesses [13]. Moreover, the adoption of AI technologies is accelerating with the objective of enhancing the stability of network services—specifically in terms of performance, quality, security, and availability—while simultaneously optimizing overall business efficiency [14]. Over the past few decades, AI and ML techniques have been increasingly leveraged to intelligently perform a variety of networking operations in future networks, from management to maintenance and protection [15]. In this context, AIOps systems emerge as a powerful approach that integrate big data analytics and ML to enhance critical IT operations such as monitoring, anomaly detection, and incident management. The emergence of new technological paradigms such as Big Data, AI, and 5G necessitates the adaptation of DevOps methodologies to accommodate evolving lifecycles and processes that extend beyond traditional software-centric solutions. This technological evolution highlights a critical contemporary challenge in AI practices, the effective operationalization of AI solutions [16]. This is the role of AIOps. By processing and analyzing the growing volume, variety, and velocity of data generated within IT environments, AIOps platforms provide actionable insights and facilitate more efficient operational decision-making. These platforms enable proactive incident detection, root cause analysis, and automated remediation, thus reducing manual intervention and improving the overall reliability and performance of IT systems. In practice, there are several different AIOps systems, with architectures designed for specific scenarios. For example, there is one dedicated to data center on-site infrastructure monitoring [17].

The ultimate objective of AIOps are to enable the development of self-healing cloud environments, in which AI-driven methodologies facilitate the real-time detection, localization, and remediation of system faults with minimal human intervention [18]. Also, AIOps possess the capability to process and analyze large-scale data streams in real time, thereby generating insights that are often beyond the reach of traditional analytical approaches.

This capacity supports more informed decision-making and enhances the effectiveness of strategic planning [19]. Using advanced ML algorithms and data-driven analytics, AIOps aim to improve operational resilience, reduce downtime, and optimize IT service management (ITSM), ultimately fostering a highly adaptive and intelligent infrastructure capable of self-regulation and continuous improvement [20]. Moreover, recent advances in the field of ML and large language models (LLM) brought this AIOps vision closer to reality [13,14]. Specifically, in recent years, large language models (LLMs) have undergone substantial advancements in both their architecture and capabilities [21]. Consequently, these models have unlocked significant opportunities for advancing downstream, domain-specific applications, like in the field of IT operations.

Despite these advances, conventional AIOps systems are limited by their reliance on predefined rules and reactive responses. They lack the autonomy needed to proactively detect and resolve incidents without human input. Here, Agentic AIOps come into play.

Agentic AIOps represent the next evolutionary step by integrating autonomous AI agents that proactively monitor, analyze, and respond to IT events in real time. Inspired by the concept of Agentic AI [22], which emphasizes goal-oriented behavior and minimal human intervention, Agentic AIOps aim to enable fully autonomous IT operations. Unlike traditional AIOps, which rely on centralized decision systems, Agentic AIOps utilize decentralized AI agents that collaborate and communicate to dynamically optimize IT environments. These agents can independently execute remediation workflows, coordinate with other agents, and continuously learn from operational data to improve efficiency and accuracy.

Although current AIOps systems have demonstrated their potential to enhance IT operations through automation and analytics, they focus primarily on observability, leveraging predefined patterns across event data, enabling understanding of problem root causes or the imminence of future incidents. Existing products such as *Watson AIOps* [23], *Splunk AIOps* [24] and *ServiceNow* [25] reflect the limitations of their capabilities related to observability.

With all of the above in consideration, there is also no canonical definition of Agentic AIOps—leading to no clear view of their standard capabilities. Hence, we see this as an emerging field that would benefit from a more strategic view on its further development direction.

We propose a vision for the future AIOps that includes automated diagnosis and, ultimately, actionability through automated resolutions and preventive actions under certain autonomy, besides as-is capabilities. Hence, a system that materializes such a vision would be able to understand problems and events, and then act by performing resolutions and preventions, respectively. As such, we describe the concept of a comprehensive framework for implementing fully autonomous and adaptive IT operations using intelligent agents. Therefore, this paper aimed to address the following research questions:

- What is our vision for the next generation of Agentic AIOps that help with maintaining IT service health by supporting IT operations, going beyond just observability, through autonomous diagnosis and resolution of incidents and problems and by preventing potential problems through proactive event management?
- What are the approaches and key architectural components required to design and implement an effective Agentic AIOps system?
- What is the line of evolution for AIOps, the potential of future development through Agentic AIOps and the core principles of a framework to ensure realization of that potential by maximizing autonomy levels in a reliable fashion?

This paper proposes a novel framework for an Agentic AIOps system by defining its core components, functionalities, and architectural requirements. The proposed framework emphasizes:

- Enablement of autonomous problem and incident management, request fulfillment, and prevention of potential issues using intelligent agents with contextual awareness and self-learning capabilities.
- Alignment to service management best practices—such as ITIL and Unified Process Framework for IT (UPF-IT)—while supporting a continuously evolving range of technologies present in organisations and real environments.
- Scalable deployment across all layers of the IT landscape, including infrastructure, middleware, data, and applications.

2. Materials and Methods

2.1. Preamble

To identify relevant studies for this article on Agentic AIOps, we have conducted a systematic review of the literature, combining academic research with industry reports. Finally, after finding more than 140 articles by searching using keywords like ‘AIOps’, ‘framework’, ‘machine learning for IT operations’, and ‘self-healing IT systems’, we set our closer attention to top cited articles from well-known databases such as IEEE Xplore, ACM Digital Library, and arXiv. In parallel, we reviewed industry white papers and technical reports from IBM, Splunk, Dynatrace, Gartner, RedHat, and Forrester, which provided insights into the practical applications and market trends of AIOps. We believe that this dual approach ensured a balanced perspective that captured both theoretical advances and real-world implementations.

The selection of studies was based on reliability, relevance, and credibility. Preference was given to empirical research, systematic reviews, and case studies that demonstrate agent-based automation in AIOps system workflows. To facilitate analysis, we categorized the selected studies into key themes such as anomaly detection, event correlation, automated remediation, and intelligent decision making.

Table 1 summarizes the main criteria used for study selection.

Table 1. Selection criteria used for the literature in our study.

Selection Criteria	Description
Publication Type	Peer-reviewed articles, industry reports, white papers
Source Databases	IEEE Xplore, ACM Digital Library, Google Scholar, Gartner, Forrester
Keywords Used	AIOps, intelligent IT automation, agent-based AIOps, ML for IT operations
Time Frame	Last five years (to ensure relevance and up-to-date findings)
Evaluation Focus	Empirical studies, case studies, systematic reviews, theoretical frameworks
Core Themes	Anomaly detection, event correlation, self-healing systems, Agentic decision-making

By structuring the research findings in this way, we were able to identify trends, gaps, and emerging challenges in the field of Agentic AIOps. This thematic classification also helped form a cohesive argument regarding the role of AI-driven agents in IT operations. By integrating both academic and industry insights, this article aimed to provide a comprehensive analysis of how agent-based AIOps are shaping the future of IT automation.

2.2. Review and Quantitative Analysis

As stated above, our systematic literature review focused on academic articles, industry reports and white papers covering the last five years. We identified more than 140 relevant articles, which were then filtered based on recency, relevance, and credibility. This resulted in a final selection of 42 high-impact studies containing key themes such as the following:

- Anomaly detection,
- Event correlation,
- Automated remediation,
- Intelligent decision-making in AIOps workflows.

2.3. Own Industry Experience, Focus Groups and Expert Discussions

Initially, we started by taking as a baseline our own experience in the IT industry, considering relevant, consecrated frameworks in IT operations, such as IBM's UPF-IT, on the one hand, as well as representative AIOps products, such as Watson AIOps and Splunk, present in real-life project delivery, on the other. To further incorporate practical perspectives, we conducted focus group discussions and semi-structured interviews with teammate IT professionals, AI researchers, and industry practitioners specializing in AIOps. These discussions explored the following:

- Current challenges in IT operations automation,
- The applicability of Agent-Based AIOps,
- Adoption barriers and proactive incident risk prediction [26],
- Future research directions.

These insights enriched the study's findings by offering qualitative depth, capturing industry perspectives on the feasibility and potential impact of autonomous AIOps agents, particularly in light of the inherent complexities associated with their design, development, evaluation, and iterative refinement [27].

2.4. Integrating Quantitative and Qualitative Insights

The integration of quantitative bibliometric analysis with qualitative expert perspectives allowed for a holistic understanding of the state of Agentic AIOps. By synthesizing these insights, we were able to perform the following:

- Identify gaps in current research,
- Assess the alignment between academic advancements and real-world implementations,
- Propose future research directions that bridge the gap between theory and practice.

Through this approach, our study provided a comprehensive, evidence-based evaluation of how agent-based AIOps systems are transforming IT automation.

2.5. Other Considerations

Moreover, a systematic study and analysis of the emerging discipline of AIOps revealed its inherent connection to Machine Learning Operations (MLOps), as both represent interrelated fields that utilize artificial intelligence (AI) to drive automation and enhance operational efficiency across distinct domains. In practice, AIOps and MLOps are emerging as best practices for leveraging artificial intelligence and machine learning to enhance IT operations and streamline machine learning workflows [28]. While AIOps focuses on intelligent management of IT operations through AI-driven monitoring, anomaly detection, and automated incident resolution, MLOps provides the methodologies and infrastructure necessary for the lifecycle management of ML models. Their convergence highlights a shared emphasis on scalability, automation, and continuous improvement, underscoring the role of AI in transforming both ITSM and ML workflows. While MLOps focus on streamlining the development, deployment, and maintenance of ML models, AIOps apply AI-driven analytics to IT operations, enabling intelligent monitoring, anomaly detection, and automated incident response. MLOps have evolved as ML has become crucial for business operations "necessitating robust frameworks for model deployment and management". In addition, MLOps have garnered increasing attention as a framework that fosters collaboration and communication between data scientists and IT operation professionals. Specifically, MLOps encompass the automation of the entire machine learning lifecycle, including model development, integration, testing, release, deployment, and the management of supporting infrastructure [29].

A key intersection between AIOps and MLOps lies in their shared emphasis on automation, scalability, and continuous improvement. MLOps provide the foundational infrastructure and best practices for managing ML workflows, including data versioning, model training, model deployment, and monitoring. To enhance the business value derived from ML solutions, the implementation of MLOps principles is essential throughout every phase of the workflow [30]. The main goal of MLOps is to create a set of procedures to quickly and efficiently creating ML models using tools, deployment flows, and work processes [31]. In contrast, AIOps utilize these ML models to process vast amounts of operational data, detect patterns, predict failures, and optimize IT system performance in real-time.

In addition, AIOps platforms increasingly incorporate MLOps principles to maintain and improve the accuracy of predictive models used for anomaly detection, root cause analysis, and proactive remediation. This convergence is essential in modern IT environments, where dynamic infrastructure and high-volume data streams require adaptive self-learning systems.

Thus, MLOps act as an enabler for AIOps, ensuring that AI models deployed in IT operations remain robust, interpretable, and continuously updated, thus enhancing the overall resilience and efficiency of ITSM [32].

MLOps can be summarized as follows:

- Focuses on the development, deployment, and lifecycle management of ML models;
- Ensures that ML models are efficiently trained, versioned, monitored, and updated;
- Includes aspects like data pipelines, model retraining, model deployment like continuous integration and continuous deployment (CI/CD), and governance. CI/CD is "the appropriate design pattern to support model-as-a-service in AIOps" [33];
- Primarily used in data science and ML applications.

Meanwhile, AIOps can be summarized as follows:

- Uses AI/ML techniques to automate and enhance IT operations;
- Focuses on real-time monitoring, anomaly detection, event correlation, and incident response in IT systems;
- Helps IT teams manage logs, metrics, alerts, and incidents using intelligent automation;
- Primarily used in DevOps, IT infrastructure management, and cybersecurity.

The key differences between AIOps and MLOps are presented in Table 2.

Table 2. MLOps vs. AIOps Comparison.

Feature	MLOps	AIOps
Primary Goal	Deliver and maintain ML models in production	Automate and enhance IT operations using AI
Scope	ML pipelines, model training, deployment, monitoring	IT observability, anomaly detection, event correlation, incident response
Data Sources	Structured datasets, feature stores, databases	Logs, metrics, traces, events, alerts from IT systems
Key Techniques	Model training, hyperparameter tuning, CI/CD for ML, versioning	Anomaly detection, predictive analytics, event correlation, NLP for log analysis
Automation Level	Partial (mostly focused on model deployment and retraining)	High (self-healing, auto-remediation, predictive issue detection)
Main Users	Data scientists, ML engineers, software engineers	IT Operations Teams, DevOps engineers, Site Reliability Engineers (SREs)
Challenges	Model drift, data drift, retraining complexity, explainability	Noisy alerts, false positives, integration with existing IT tools, trust in automation
Key Tools and Frameworks	MLflow, Kubeflow, TensorFlow Extended (TFX), Airflow	Splunk AIOps, Dynatrace, New Relic, IBM Watson AIOps, Moogsoft
End Goal	Deliver high-performing ML models that improve business outcomes	Reduce Mean Time to Resolution (MTTR), enhance IT system reliability, automate incident management

3. Results

Generative AI (GenAI) opened up a realm of application opportunities in certain key domains, one of which is IT Operations [34]. Enterprises need to run their services while maintaining service levels that measurably address operational aspects of the systems, such as the following:

- Availability, as the ability of the service to serve client requests a certain percentage of the time, typically measured as a percentage applied to a time period;
- Resilience, as the ability of the service to continuously operate even in conditions of (natural) disasters that may affect certain sites of its deployment. Indicators such as Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are subsumed into this service aspect;
- Performance, which measures certain qualities related to response times and throughput, related to transaction processing;
- Capacity, which is the ability to accommodate a certain volume, such as concurrent user sessions or an amount of data;
- Scalability, as the trait allowing the service to accommodate additional load requiring less than linear addition in its underlying infrastructure;
- Security;
- Maintainability, which refers to allowing the service to be patched or upgraded.

An IT service is a set of components that is 'commissioned' by its client. Simply put, it can be an application system and/or its middleware and/or its infrastructure. For example, when a client uses virtual machines or containers from Cloud, it is that infrastructure that constitutes the service (as Infrastructure-as-a-Service); whilst the respective cloud platform is the provider. Another example is an enterprise that uses an Enterprise Resource Planning (ERP) system deployed on its premises, in which case the aforementioned ERP is the service while the team that performs related operations is the provider—it can be an external vendor or an internal IT department.

Gartner introduced the term Algorithmic IT Operations in 2017 [35], which was a precursor to (predictive) Artificial Intelligence for IT Operations (see Figure 1). From the definition, "AIOps platform technologies comprise of multiple layers that address data collection, storage, analytical engines and visualization. They enable integration with other applications via application programming interfaces (APIs), allowing for a vendor-agnostic data ingestion capability. Therefore, AIOps platforms can seamlessly interact with IT operations management tools (ITOM) toolsets because of the ability to deal with data from any tool regardless of the data type", we see the focus on observability of the health of IT services, creating the foundation of event data processing. Later, the current AIOps made its more academic debut [36].

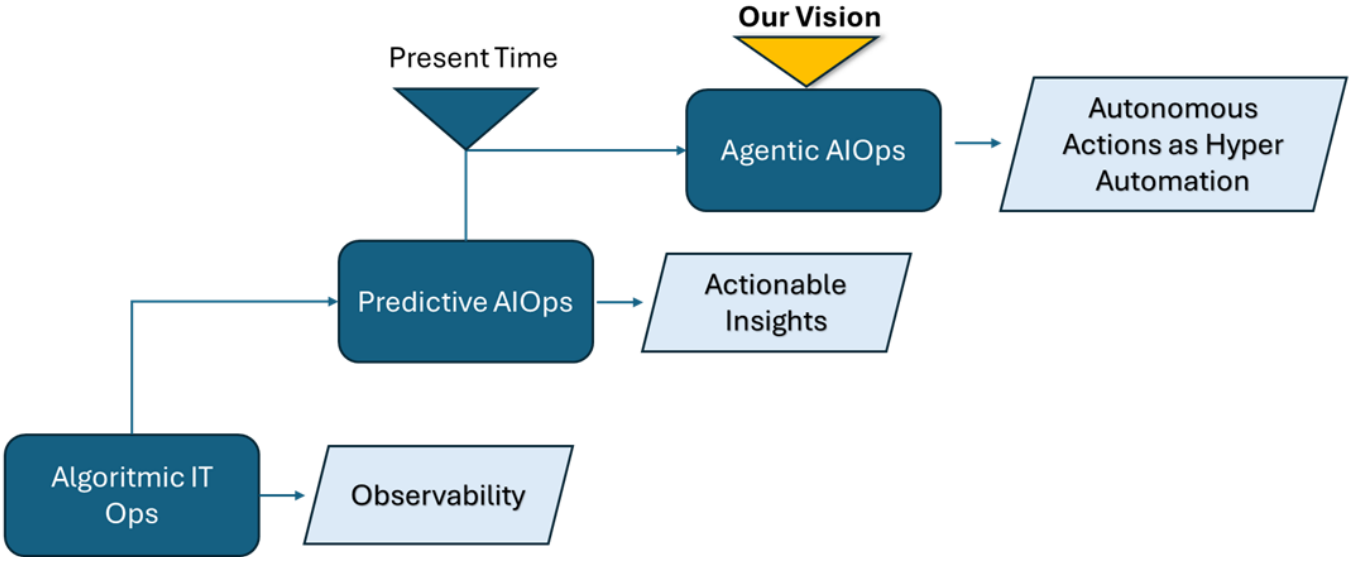

Figure 1. Evolution of AIOps.

3.1. AIOps Evolution to Date

Early AIOps approaches focused on processing incident and problem data and reports, allowing for an aggregated view of the respective data points, on the one hand, and better planning for the processing and resolution of tickets, on the other [37]. It was, at the time, a natural data analytics application in the IT Operations domain. Subsequent evolution introduced Predictive AIOps that help detect proactively imminent incidents and problems from current event data. For example, considering past experience, applications running on a server running above 70% CPU utilization usually see steep performance degradation as that threshold gets passed. If such a condition occurs, the AIOps management system might issue an alert in the system administration console, which then becomes actionable by the responsible human or system actor [38]. In another real-life example, when a performance metric—such as latency—exceeds a predefined threshold, an alert is automatically generated to notify on-call engineers. These real-time notifications facilitate prompt diagnosis and resolution of system issues [39]. However, the decision on if, when and how to act (i.e., resolution implementation) is left to the Operations team.

We witness a further evolution, from observability to predictive operational insights (see Figure 1), which is presently materialized in products across the industry (such as Watson AIOps) that assist in determining and preventing future issues. The next phase of AIOps, in our vision, is about introducing automation for understanding issues (problems and incidents) and then the automation for solving them—on the one hand—as well as the ability to anticipate imminent problems and preventive actions—on the other. These capabilities would build on the as-is for dispatching alerts, as a foundation.

Therefore, a key aspect to consider in this context is the level of automation, which can be looked at from two perspectives:

- Scope—we see an indication of proactive preventive actions implemented within the AIOps notion space [38];
- Level of autonomy.

Level 1: the human operator performs the task and turns it over to the computer to implement.

Level 2: the computer helps to determine the options.

Level 3: the computer determines and suggests options. The human operator can choose to follow the recommendation.

Level 4: the computer selects the action and the human operator decides if it should or should not be done.

Level 5: the computer selects the action and implements it if the human operator approves the action.

Level 6: the computer selects the action and informs the operator in case the operator wants to cancel the action. Four additional levels refer to communication between the operator and the autonomous device.

Level 7: the computer performs the action and tells the human operator what it did.

Level 8: the computer performs the action and tells the human only if the human operator asks.

Level 9: the computer performs the action when told and tells the human operator only if the computer decides the operator should be told.

Level 10: The computer performs the action if it decides that it should be performed. The computer tells the human operator only if it decides the operator should be told [40].

Our framework establishes a progressive implementation model for autonomy advancement, allowing organizations to evolve their Agentic AIOps capabilities through defined maturity stages. Rather than advocating for immediate full autonomy, this approach enables IT departments to strategically deploy autonomous components at carefully calibrated levels that align with their specific risk tolerance profiles, governance requirements, and operational readiness. Organizations can begin with lower autonomy levels in less critical domains, where agents provide recommendations but require human approval before action, and then progressively expand both the autonomous agents' scope and decision authority as confidence and performance data accumulate.

In our view, the evolution of AIOps corresponds to the journey from observability to Closed-Loop IT Operations, in terms of capabilities [41].

Figure 1 illustrates the progressive evolution of the AIOps capabilities and results. It begins with foundational observability and analytics, advances to the current state of enhanced incident visibility, and ultimately converges on Agentic AIOps, a paradigm in which, in our vision, AI-driven agents autonomously perform diagnosis, resolution, and proactive prevention of IT incidents.

3.2. Service Management Alignment

IT Operations is the domain of application for AIOps and a subset of ITSM, whose best practices are embodied in ITIL [2]. ITIL's approach is more to lay out the principles and practices of Service Management, deferring a definition of actual workflows and work products to the industry. That is for a good reason, given the fact that ITIL was not intended to go to that level of detail—leaving room for flexibility for the organizations that adopt the framework—and that not all practices in ITIL can rely on canonical workflows. This might be the reason why ITIL version 4 replaced processes in version 3 with practices. The ITIL framework conceptualizes the service lifecycle as comprising five distinct stages, each serving as a structured grouping for a set of well-defined practices or processes:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continuous service improvement [42]

The consumer entity, organization or individual commissions the service once it completes the 'transition', thus becoming 'operational'. The Service Operation corresponds essentially to IT Operations, comprising processes such as the following:

- Event Management
- Incident Management
- Request Fulfillment
- Access Management
- Problem Management
- IT Operations Control
- Facilities Management
- Application Management
- Technical Management

Looking at them, we realize that a good part of them can be standardized, and hence, well-defined process workflows can be defined for them, providing the foundation for automation. Indeed, this was the purpose of IBM's Process Reference Model for IT (PRM-IT), part of UPF-IT, which is closely aligned with ITIL [43], augmenting it by adding actual workflows to the processes (practices) defined by ITIL, and conceiving a supplementary set of processes. This enabled the company to standardize and automate IT operations for the purpose of economic benefits in this field, which constitutes a major line of business.

A view on how IT Services, Operations, PRM-IT, and AIOps scopes relate to each other is presented in Figure 2.

Overall, our study results suggested that further evolution of AIOps into 'Agentic' AIOps would introduce radically new capabilities for the following:

- Automated understanding of existing incidents and problems as well as for potential, imminent ones.
- Automated applications for resolutions and preventive actions in addition to the current ones in the literature and industry, which are essentially limited to operational insights generation.

Considering, on the other hand, the service management activities continuum, those capabilities would need to fully align with ITIL (via UPF-IT) in order to comprehensively support the relevant IT Operations.

This led us to articulate our vision for the Agentic AIOps, which we elaborate on in the next section.

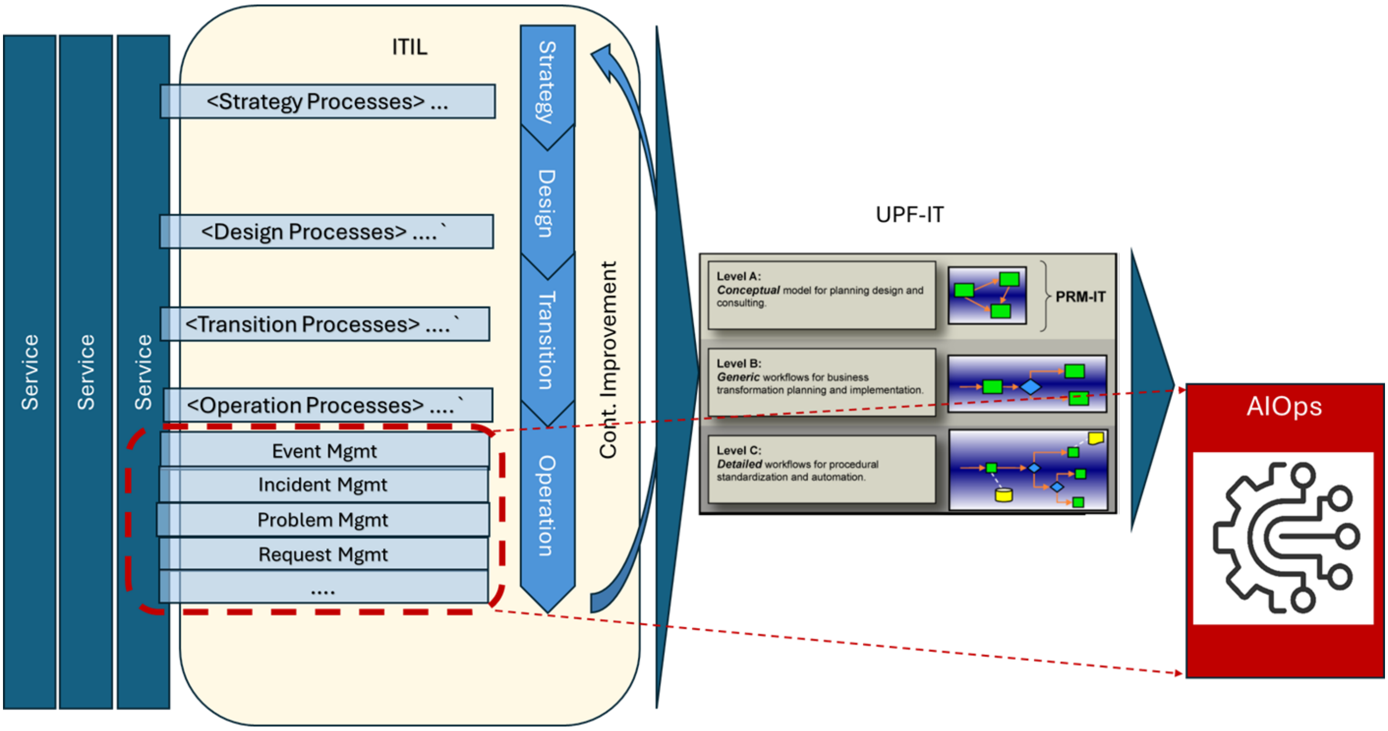
Service
Service
Service
ITIL
<Strategy Processes> ...
<Design Processes> ....`
<Transition Processes> ....`
<Operation Processes> ....`
Event Mgmt
Incident Mgmt
Problem Mgmt
Request Mgmt
....
Strategy
Design
Transition
Operation
Cont. Improvement
UPF-IT
Level A:
Conceptual model for planning design and consulting.
PRM-IT
Level B:
Generic workflows for business transformation planning and implementation.
Level C:
Detailed workflows for procedural standardization and automation.
AIOps

Figure 2. IT Ops versus ITSM and AIOps.

4. Discussion

As we noted in the Introduction, there is no standard definition for Agentic AIOps in the literature. Therefore, we propose the following definition: An Agentic AIOps system is an IT system that supports IT Operations, in full alignment with ITIL Service Operation practice, providing capabilities for automated understanding of requests, incidents, problems, and events, decisions about the course of action, as well as performing actual actions required for fulfilling requests and resolve issues, with automation enabled by specialized agents operating at different levels of autonomy.

In the following, we introduce an Agentic AIOps development framework designed to articulate the system architecture and inform its ongoing development, with the objective of ensuring sustained evolution and adaptability within complex and dynamic IT environments.

4.1. Proposed Framework Overview

Figure 2 tells us an interesting story. If ITIL is the body of knowledge with regards to ITSM, that includes IT Operations.

The operations processes in ITIL are those processes dedicated to running and maintaining 'operational' services, i.e., services that were 'strategized', 'designed' then 'transitioned' to operations. These processes define the operational scope of IT management and, consequently, delineate the functional boundaries of AIOps. ITIL represents a mature and refined framework of best practices for delivering IT services, so we do not look for an opportunity to replace it with something better (e.g., proposing new or different processes to manage IT services). PRM-IT defines the flows for comprising activities, tasks, and work products for each ITIL process, then extends ITIL with some processes. The role of AIOps should be to take those ITIL processes for operations and (hyper)automate them using AI, leveraging the flows defined by PRM-IT. Current AIOps mainly address the observability aspect, ultimately including insights that help prevent issues. The integration of artificial intelligence into the DevOps lifecycle enables organizations to extract actionable insights from heterogeneous data sources, automate repetitive processes, proactively identify and address operational anomalies, and enhance overall system performance, improving operational efficiency [44]. On the other hand, current automation is limited to certain DevOps enablement (i.e., automation components typically launched by human operators in the appropriate context).

Our vision encompasses the entire progression from raw event and incident data to its systematic dissemination, followed by automated diagnosis, and ultimately leading to fully autonomous resolution and proactive prevention. The adoption of such a fully automated AIOps platform may facilitate the evolution of traditional Continuous Integration/Continuous Deployment (CI/CD) pipelines into more advanced Continuous Integration, Continuous Deployment, Continuous Monitoring, and Continuous Correction (CI/CD/CM/CC) frameworks [45], thereby extending automation across the entire software delivery lifecycle.

With all of the above in mind, this means that we can find the way of establishing an AIOps framework that allows for a comprehensive automation of understanding and resolving (potential) issues in an IT environment, by aligning with ITIL through the means of an actionable process reference model such as PRM-IT, which is part of UPF-IT.

The process model dimension allows us to identify all possible standard IT Operations activities that would enable us to select those candidates for automation through Agentic AIOps system components.

The second dimension of our proposed framework consists of the very scope of the IT Operations, that is, the services themselves as they are found in the catalog of the given consumer:

- Actual applications;
- Platform services such as middleware, runtimes, or databases;
- Infrastructure, in terms of server, storage, and network.

This can use as a reference the NIST Definition of Cloud Computing (SP 800-145) [46], which is actually applicable for on-premise services as well as cloud services. The representation of IT services in Figure 3 indicates that the layer above encapsulates the one below, that is, the Platform encapsulates the underlying infrastructure, for example, a database service encapsulates the servers on which the database process is deployed and runs.

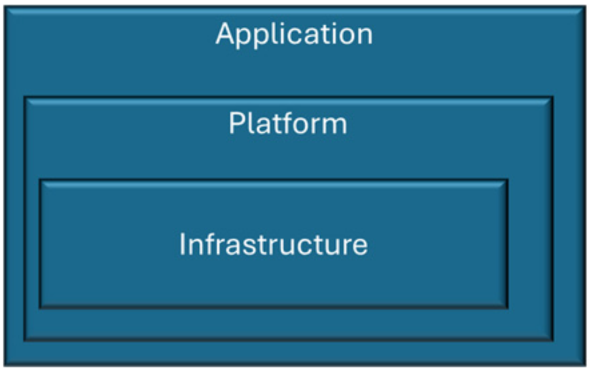

Figure 3. IT Service Illustration.

The third dimension is the AIOps system capability needed to achieve a closed-loop environment, from understanding the current state and evolutionary tendencies to deciding the course of action, either to prevent future problematic conditions or to address them in actuality, through performing subsequent actions automatically and with an assumed level of autonomy. We see that the definition of a framework that considers all of the above aspects is feasible (see Figure 4), while also including the integration aspect.

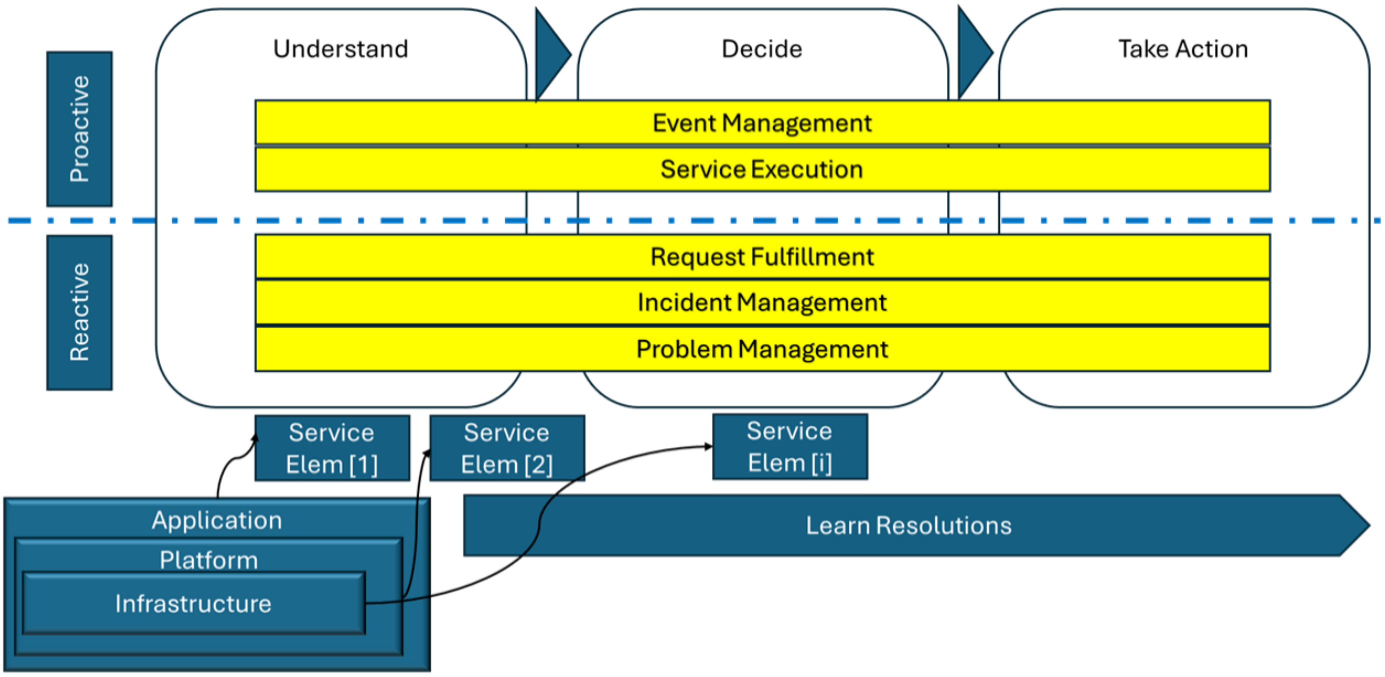

Figure 4. Overview of the Agentic AIOps Development Framework.

Our framework states that a comprehensive Agentic AIOps needs to have in scope the Operations Service Lifecycle ITIL processes (shown in yellow in Figure 4). Each of these processes will involve one or more Service Elements, where there is either a concrete application, a platform (e.g., Oracle WebLogic), or a given Operating System (e.g., Linux). For example, the incident management process needs to be able to provide resolutions for WebLogic JEE outages or for Linux operating system issues in general for all Service Elements in the environment, for which a taxonomy needs to be developed. For each process, a mapping to components should be completed, such as the one in the following Incident Management example, in order to specify the components of the system.

We notice that the 'Understand', 'Decide' and 'Take Action' high-level phases provide a foundation for deciding the technical capability or components to employ for realization.

As a first remark, we included in the framework the UPF-IT processes that are applicable to AI implementation as opposed to just traditional automation. That is the reason why we included Event Management, Service Execution, Request Fulfillment, Incident Management, and Problem Management and excluded Identity and Access Management and Data Management. All of the included processes follow the understand–decide–take action model, with the first two materializing the proactive perspective of such a system while the other three embody its reactive perspective. This system should be able to learn applicable resolution in order to implement its 'Take Action' phase and work with all service elements in the environment, where any service element is integral to an application, platform, or infrastructure.

4.2. Incident Management Example

As an example, we may look at Figure 5, where we consider the incident management process as per UPF-IT.

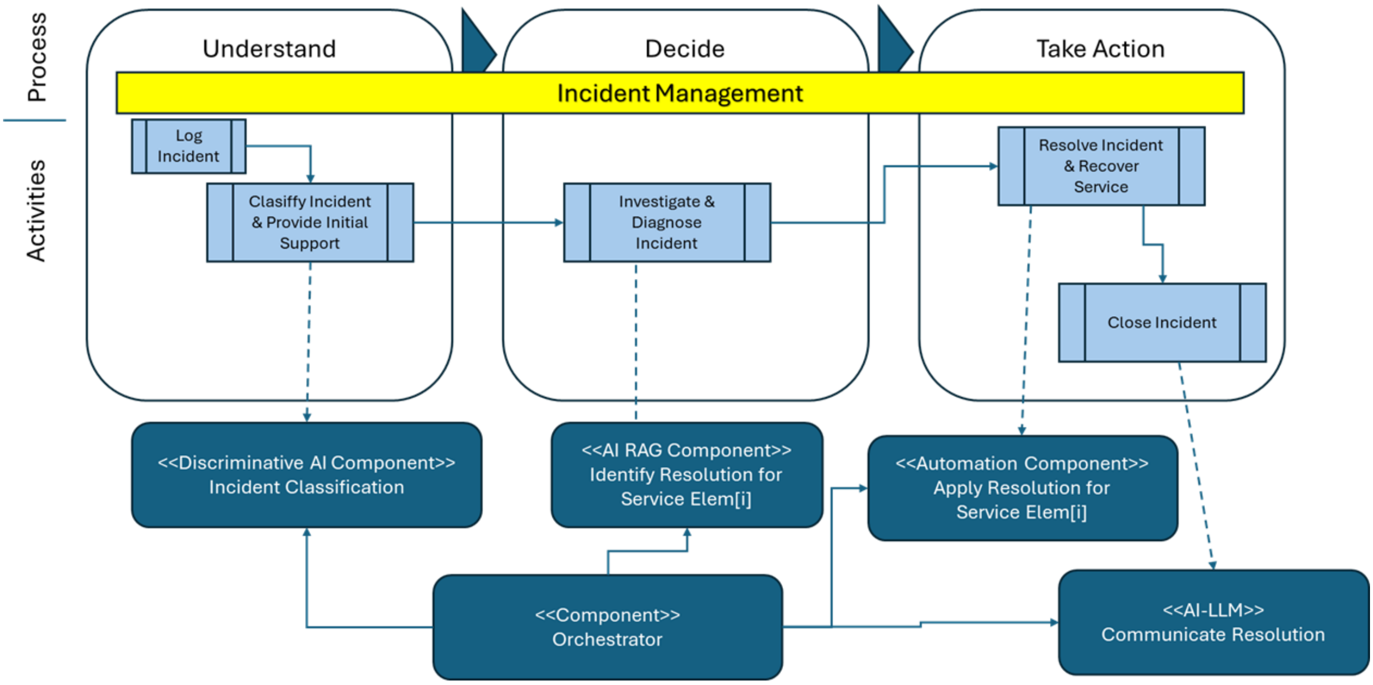
Process
Activities
Understand
Decide
Take Action
Incident Management
Log Incident
Clasiffy Incident & Provide Initial Support
Investigate & Diagnose Incident
Resolve Incident & Recover Service
Close Incident
<<Discriminative AI Component>> Incident Classification
<<AI RAG Component>> Identify Resolution for Service Elem[i]
<<Automation Component>> Apply Resolution for Service Elem[i]
<<Component>> Orchestrator
<<AI-LLM>> Communicate Resolution

Figure 5. Incident Management Example for System Component Mappings.

Based on the incident management flow, as per PRM-IT, we identified the activities that constitute the scope of the next Agentic AIOps system.

Starting from the process flow, we map the steps on the *Understand*, *Decide*, and *Take Action* phases in order to identify the appropriate system capability to support that step.

- 'Log Incident' and 'Classify Incident and Provide Initial Support' refer to 'Understand'. As such, we can design and implement a discriminative AI component to classify the incident and then identify the concerned service element, e.g., a MS SQL Server database.
- The 'investigate and diagnose incident' has the goal of identifying what caused it, for example, an exhausted storage volume. That diagnosis can be performed using an AI retrieval augmented generation (RAG) component. This is a 'decision' element, as such.
- 'Resolve Incident and Recover Service' ultimately 'Takes Action' and applies the resolution that can be realized by an automation component, such as a Jenkins pipeline that contains steps to extend the concerned storage volume and then starts the SQL Service.
- Finally, the dispatch and 'close incident' updates the status of the ticket communication, potentially employing an AI-LLM component.

The orchestrator component has the responsibility of controlling the flow across the other components mentioned above.

4.3. Considerations on Research Questions

This section explicitly addresses how our proposed Agentic AIOps framework aligns with and answers the research questions in the Introduction. By mapping our findings and framework components to each question, we comprehensively evaluate how the proposed approach advances the field of autonomous IT operations.

RQ1: What is our vision for the next generation Agentic AIOps that helps maintain IT service health by supporting IT operations, going beyond just observability, through autonomous diagnosis and resolution of incidents and problems and by preventing potential problems through proactive event management?

The proposed framework addresses this question by establishing a comprehensive approach to the management of autonomous IT services across the full spectrum of operational activities. As demonstrated in Section 3.1, the evolution of AIOps capabilities from observability to closed-loop automation provides the foundation for autonomous service health management. Our framework extends this evolution through explicit alignment to ITIL via UPF-IT. This leads, for example, to features like the following:

- Proactive Event Management: The framework enables the continuous monitoring and analysis of system events using AI-powered components that can detect patterns indicative of potential service degradation before they impact users. By mapping event management processes to the "Understand" phase of our framework, we enable early detection of anomalies across all service layers (infrastructure, platform, and application).
- Autonomous diagnosis: In the "Decision" phase, the framework takes advantage of advanced AI techniques such as knowledge-based systems and RAG to diagnose the root causes of incidents. This capability, demonstrated in our incident management example in Figure 5, allows the system to accurately determine the nature of the problem without human intervention.
- Self-Healing Actions: Our framework's "Take Action" phase enables autonomous remediation through predefined automation workflows. As illustrated in our example, when a database incident occurs due to storage exhaustion, the system can independently deploy the appropriate resolution by extending storage and restarting the necessary services.

This multilayered approach ensures that IT service health is maintained through a combination of preventive detection, accurate diagnosis, and autonomous resolution, significantly reducing the need for human intervention in routine operational issues.

RQ2: What are the key architectural components required for an effective Agentic AIOps system?

Our framework helps identify essential architectural components through mapping to activity or task, capability—according to the Understand–Decide–Take Action paradigm—and technology/service element. Taking into account the incident management example in Figure 5, we have outlined the following:

- The Orchestrator component manages the control flow through the other components, end-to-end, as per the Incident Management process flow (as depicted by the process elements in the figure).
- 'Understand' capability components.

The incident Classification 'Discriminatory AI' component in our example implements automated classification of incidents using—in this instance—a discriminatory AI model.

- Identify capability components.

Identify the resolution for the <Service Elem[i]> component. Once the root cause has been identified by the previous component, at the level of the <Service Elem[i]> (an MS SQL database, for instance, that might have run out of space), this component finds a resolution learned from previous experience. It determines the parameters to be passed to this resolution. This allows the orchestrator to invoke the respective automation component (see next).

- 'Take Action' capability components.

‘Apply Resolution for <Service Elem[i]>’ can be an automation component, such as an Ansible playbook that performs the resolution steps (e.g., extends the database storage volume). Communication resolution handles communication to requestors as part of the incident closure.

We notice that we can develop a comprehensive, autonomous system by instituting the above approach for all processes for all technologies in alignment with the service elements in a given environment.

RQ3: What are the core principles for maximizing autonomy levels in a reliable fashion?

Our framework establishes several core principles for achieving higher levels of autonomy while maintaining operational reliability.

- Progressive Autonomy: Referring to the ten levels of autonomy described in Section 3.1, our framework advocates a progressive approach to increasing autonomy. Organizations can implement Agentic AIOps components at different autonomy levels based on risk tolerance and operational maturity.
- Process Standardization: The framework’s alignment with established ITIL/UPF-IT processes ensures that autonomy is constructed upon standardized operational practices, reducing the risk of unexpected behaviors while enabling consistent automation across domains.
- Service-aware design: By incorporating service layer awareness, the framework ensures that autonomous actions consider the hierarchical nature of IT services, preventing remediation actions that might resolve issues at one layer while creating problems at another.
- Continuous Learning: The framework includes feedback loops that allow the system to learn from the outcomes of autonomous actions, gradually improving the accuracy of its decisions and the effectiveness of its remediation strategies.
- Human Oversight: While maximizing autonomy, the framework maintains provisions for human oversight at critical decision points, particularly for high-risk actions or unprecedented scenarios, ensuring that reliability is not compromised in pursuit of autonomy.

5. Conclusions

AIOps, with their ultimate evolutionary level of Agentic AIOps, represent a ‘young’ domain that certainly opens significant innovation opportunities. We have hereby provided a definition as a foundation for further research and development. As such, we see the place of a framework to help with planning and managing the development of a comprehensive Agentic AIOps system.

Our research contributes significantly by integrating established ITSM frameworks with emerging AI agent technologies to address critical operational challenges. Our three-dimensional framework, aligning process models, service elements, and autonomous capabilities, provides a structured pathway from current observability-focused solutions to truly autonomous IT operations. Unlike existing approaches that primarily detect anomalies, our framework enables autonomous diagnosis and remediation with minimal human intervention.

We mentioned here the key concepts and principles of such a framework in an attempt to lay out the foundation for its actual elaboration in subsequent efforts. In particular, the key features derived are as follows:

- Full alignment with ITIL—via UPF-IT—process flows to provide full coverage of IT Operation activities;
- Establishment of an IT Service taxonomy, including Service Elements featuring distinct technologies for infrastructure, middleware, and applications;

- Application of *the understand–decide–take action* paradigm for allowing consistent architectural decision making for component realization (such as various AI models versus automation implementations);
- Continuous training of the target Agentic AIOps system in order to maximize its proactive posture.

Our main future research directions will focus on:

- Defining the capabilities of the system for a given process. Indeed, any ITIL Operations process can be seen as requiring its own solution (or system capability);
- Specifying components for a given technology—infrastructure, middleware, and application—for a certain process element, such as an activity or task. Considerations such as AI model types and related implementation guidelines apply;
- A conceptual architecture will be proposed to support specific aspects of the aforementioned directions, which are discussed in a dedicated chapter.

Although our framework presents a forward-looking vision for Agentic AIOps, we recognize certain limitations. First, we remark that currently we do not have experimental results that materialize the presented view, since it is a vision of the future of Agentic AIOps. This represents an opportunity for future research to empirically test these concepts. Second, we also remark on the fact that security concerns are not considered in the scope of our paper, since those aspects need to be considered in the Security Management process and Security Management Framework of the organization in their own right, while the Agentic AIOps system needs to be covered from a development and operational perspective, alongside all the other systems in the environment.

Implementing Agentic AIOps systems raises important ethical and governance considerations that must be addressed for responsible deployment. As autonomous agents gain greater decision-making authority over critical IT infrastructure, organizations must establish clear accountability frameworks that define the boundaries of responsibility between human operators and AI systems. This includes implementing transparency mechanisms that provide visibility into the rationale for agent decision making, particularly for critical remediation actions. Additionally, organizations should develop appropriate oversight structures with defined escalation paths for scenarios where autonomous actions could have significant business impacts. From a governance perspective, we recommend establishing formal review processes for autonomous agent capabilities before deployment to production environments and continuous monitoring of agent performance against established key performance indicators (KPIs). The process of selecting specific KPIs also helps in defining a continuous process of enhancements [47]. As Agentic AIOps mature, industry-wide standards for ethical implementation will become increasingly essential to ensure responsible adoption that balances operational efficiency with appropriate human oversight.

Author Contributions: Conceptualization, R.D.Z. and C.B.; Formal analysis, C.B.; Investigation, C.B. and R.C.; Methodology, R.D.Z.; Resources, R.D.Z., C.B. and R.C.; Supervision, R.D.Z.; Validation, R.D.Z. and R.C.; Visualization, C.B. and R.C.; Writing—original draft, C.B.; Writing—review & editing, R.D.Z., C.B. and R.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors would like to express their gratitude to the administrative staff at Research Center of Bucharest University of Economic Studies for their invaluable support in facilitating the research process.

Conflicts of Interest: Author Corneliu Bărbulescu was employed by the company IBM. Moreover, author Corneliu Barbulescu did not use IBM data, did not receive funding and has no other business relationship with IBM regarding the content of the article submitted for publication. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
AIOps	Artificial Intelligence for IT Operations
CI/CD	Continuous integration/Continuous deployment
DevSecOps	Development, security and operations
ERP	Enterprise Resource Planning
GenAI	Generative Artificial Intelligence
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITOA	IT Operations Analytics
ITSM	IT Service Management
KPIs	Key Performance Indicators
LLMs	Large Language Models
MLOps	Machine Learning for IT Operations
NIST	National Institute of Standards and Technology
PRM-IT	Process Reference Model for IT
RAG	Retrieval augmented generation
RPO	Recovery Point Objective
RTO	Recovery Time Objective
UPF-IT	Unified Process Framework for IT

References

1. Notaro, P.; Cardoso, J.; Gerndt, M. A Systematic Mapping Study in AIOps. In *Service-Oriented Computing—ICSOC 2020 Workshops*; Hacid, H., Outay, F., Paik, H., Alloum, A., Petrocchi, M., Bouadjenek, M.R., Beheshti, A., Liu, X., Maaradji, A., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2021; Volume 12632, pp. 110–123, ISBN 978-3-030-76351-0.
2. ITIL V3. Available online: https://www.itsm-docs.com/blogs/itil-faq/itil-v3 (accessed on 10 March 2025).
3. Dande, F.; Li, X.; Shofoluwe, M.; McLeod, A. Artificial Intelligence Integration in IT Service Management: An ITIL Configuration Management Process Review. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Detroit, MI, USA, 9–11 October 2024; IEOM Society International: Detroit, MI, USA, 2024.
4. Iden, J.; Eikebrokk, T.R. Implementing IT Service Management: A systematic literature review. *Int. J. Inf. Manag.* **2013**, *33*, 512–523. [CrossRef]
5. Remil, Y.; Bendimerad, A.; Mathonat, R.; Kaytoue, M. AIOps Solutions for Incident Management: Technical Guidelines and A Comprehensive Literature Review. *arXiv* **2024**, arXiv:2404.01363.
6. Shen, S.; Zhang, J.; Huang, D.; Xiao, J. Evolving from Traditional Systems to AIOps: Design, Implementation and Measurements. In Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA), Dalian, China, 25–27 August 2020; IEEE: Dalian, China, 2020; pp. 276–280.
7. How To Get Started with Aiops. Available online: https://www.gartner.com/smarterwithgartner/how-to-get-started-with-aiops (accessed on 17 April 2025).
8. Bogatinovski, J.; Nedelkoski, S.; Acker, A.; Schmidt, F.; Wittkopp, T.; Becker, S.; Cardoso, J.; Kao, O. Artificial Intelligence for IT Operations (AIOPS) Workshop White Paper. *arXiv* **2021**, arXiv:2101.06054.
9. Lyu, Y.; Rajbahadur, G.K.; Lin, D.; Chen, B.; Jiang, Z.M. Towards a Consistent Interpretation of AIOps Models. *ACM Trans. Softw. Eng. Methodol.* **2022**, *31*, 1–38. [CrossRef]
10. Dang, Y.; Lin, Q.; Huang, P. AIOps: Real-World Challenges and Research Innovations. In Proceedings of the 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), Montreal, QC, Canada, 25–31 May 2019; IEEE: Montreal, QC, Canada, 2019; pp. 4–5.

11. Kumar, S. Data Silos A Roadblock for AIOps. *arXiv* **2023**, arXiv:2312.10039.
12. Yang, X.; Palmes, P.; Jha, S.; Turkkan, B.; Vanloo, G.; Bagehorn, F.; Narayanaswami, C.; Shwartz, L.; Abe, N.; Deng, Y.; et al. SAM: Subseries Augmentation-Based Meta-Learning for Generalizing AIOps Models in Multi-Cloud Migration. In Proceedings of the 2024 IEEE 17th International Conference on Cloud Computing (CLOUD), Shenzhen, China, 7–13 July 2024; IEEE: Shenzhen, China, 2024; pp. 291–301.
13. Mao, H.; Zhang, T.; Tang, Q. Research Framework for Determining How Artificial Intelligence Enables Information Technology Service Management for Business Model Resilience. *Sustainability* **2021**, *13*, 11496. [CrossRef]
14. Min, S.; Kim, B. AI Technology Adoption in Corporate IT Network Operations Based on the TOE Model. *Digital* **2024**, *4*, 947–970. [CrossRef]
15. Benzaid, C.; Taleb, T. AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions. *IEEE Netw.* **2020**, *34*, 186–194. [CrossRef]
16. de Arcaya, J.D. A Framework for the Operationalization of Analytic Workloads in Complex Distributed Computing Environments. Ph.D. Thesis, Universidad de Deusto, Bilbao, Spain, 2024.
17. Dong, W. AIOps Architecture in Data Center Site Infrastructure Monitoring. *Comput. Intell. Neurosci.* **2022**, *2022*, 1988990. [CrossRef]
18. Chen, Y.; Shetty, M.; Somashekar, G.; Ma, M.; Simmhan, Y.; Mace, J.; Bansal, C.; Wang, R.; Rajmohan, S. AIOpsLab: A Holistic Framework to Evaluate AI Agents for Enabling Autonomous Clouds. *arXiv* **2025**, arXiv:2501.06706.
19. Duan, Y.; Bao, H.; Bai, G.; Wei, Y.; Xue, K.; You, Z.; Zhang, Y.; Liu, B.; Chen, J.; Wang, S.; et al. Learning to Diagnose: Meta-Learning for Efficient Adaptation in Few-Shot AIOps Scenarios. *Electronics* **2024**, *13*, 2102. [CrossRef]
20. Potts, W.C.; Carver, C. Best Practices Implementing AIOps in Large Organizations. In Proceedings of the 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), Harrisonburg, VA, USA, 28–30 May 2024; IEEE: Harrisonburg, VA, USA, 2024; pp. 1–5.
21. Liu, Y.; Pei, C.; Xu, L.; Chen, B.; Sun, M.; Zhang, Z.; Sun, Y.; Zhang, S.; Wang, K.; Zhang, H.; et al. OpsEval: A Comprehensive IT Operations Benchmark Suite for Large Language Models. *arXiv* **2024**, arXiv:2310.07637.
22. Pounds, E. What Is Agentic AI? *NVIDIA Blog* 2024. Available online: https://blogs.nvidia.com/blog/what-is-agentic-ai/ (accessed on 17 April 2025).
23. IBM Watson AIOps 2.1. Available online: https://www.ibm.com/docs/en/watson-aiops/2.1?topic=overview-component (accessed on 2 April 2025).
24. Onkamo, M.; Rahman, T. Artificial Intelligence for IT Operations—Basic Guide to Start with AIOps. 2023. Available online: https://doi.org/10.13140/RG.2.2.20295.16803 (accessed on 19 February 2025).
25. Ayub, K.; Alshawa, R. A Novel AI Framework for WBAN Event Correlation in Healthcare: ServiceNow AIOps approach. In Proceedings of the 2024 IEEE Workshop on Microwave Theory and Technology in Wireless Communications (MTTW), Riga, Latvia, 2–4 October 2024; IEEE: Riga, Latvia, 2024; pp. 55–60.
26. Ahmed, S.; Singh, M.; Doherty, B.; Ramlan, E.; Harkin, K.; Bucholc, M.; Coyle, D. An Empirical Analysis of State-of-Art Classification Models in an IT Incident Severity Prediction Framework. *Appl. Sci.* **2023**, *13*, 3843. [CrossRef]
27. Shetty, M.; Chen, Y.; Somashekar, G.; Ma, M.; Simmhan, Y.; Zhang, X.; Mace, J.; Vandevoorde, D.; Las-Casas, P.; Gupta, S.M.; et al. Building AI Agents for Autonomous Clouds: Challenges and Design Principles. In Proceedings of the ACM Symposium on Cloud Computing, Redmond, WA, USA, 20–22 November 2024; ACM: Redmond, WA, USA, 2024; pp. 99–110.
28. Korada, L. AIOps and MLOps: Redefining Software Engineering Lifecycles and Professional Skills for the Modern Era. *J. Eng. Appl. Sci. Technol.* **2023**, *271*, 2–7. [CrossRef]
29. Díaz-de-Arcaya, J.; Torre-Bastida, A.I.; Miñón, R.; Almeida, A. Orfeon: An AIOps framework for the goal-driven operationalization of distributed analytical pipelines. *Future Gener. Comput. Syst.* **2023**, *140*, 18–35. [CrossRef]
30. Battina, D.S. An intelligent devops platform research and design based on machine learning. *Novat. Publ. Int. J. Innov. Eng. Res. Technol.* **2019**, *6*, 68–75.
31. Amrit, C.; Narayanappa, A.K. An analysis of the challenges in the adoption of MLOps. *J. Innov. Knowl.* **2025**, *10*, 100637. [CrossRef]
32. Diaz-de-Arcaya, J.; Torre-Bastida, A.I.; Zárate, G.; Miñón, R.; Almeida, A. A Joint Study of the Challenges, Opportunities, and Roadmap of MLOps and AIOps: A Systematic Survey. *ACM Comput. Surv.* **2024**, *56*, 1–30. [CrossRef]
33. Chen, R.; Pu, Y.; Shi, B.; Wu, W. An automatic model management system and its implementation for AIOps on microservice platforms. *J. Supercomput.* **2023**, *79*, 11410–11426. [CrossRef]
34. Feuerriegel, S.; Hartmann, J.; Janiesch, C.; Zschech, P. Generative AI. *Bus. Inf. Syst. Eng.* **2024**, *66*, 111–126. [CrossRef]
35. Gartner Says Algorithmic IT Operations Drives Digital Business. Available online: https://www.gartner.com/en/newsroom/press-releases/2017-04-11-gartner-says-algorithmic-it-operations-drives-digital-business (accessed on 17 April 2025).
36. Wu, X.; Zhang, Y.; Shi, M.; Li, P.; Li, R.; Xiong, N.N. An adaptive federated learning scheme with differential privacy preserving. *Future Gener. Comput. Syst.* **2022**, *127*, 362–372. [CrossRef]

37. Ahmed, S.; Singh, M.; Doherty, B.; Ramlan, E.; Harkin, K.; Coyle, D. AI for Information Technology Operation (AIOps): A Review of IT Incident Risk Prediction. In Proceedings of the 2022 9th International Conference on Soft Computing & Machine Intelligence (ISCMI), Toronto, ON, Canada, 26–27 November 2022; IEEE: Toronto, ON, Canada, 2022; pp. 253–257.
38. Sivakumar, S. Agentic AI in Predictive AIOps: Enhancing IT Autonomy and Performance. *Int. J. Sci. Res. Manag. IJSRM* **2024**, *12*, 1631–1638. [CrossRef]
39. Zha, J.; Shan, X.; Lu, J.; Zhu, J.; Liu, Z. Leveraging Large Language Models for Efficient Alert Aggregation in AIOPs. *Electronics* **2024**, *13*, 4425. [CrossRef]
40. Gulenko, A.; Acker, A.; Kao, O.; Liu, F. AI-Governance and Levels of Automation for AIOps-supported System Administration. In Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; IEEE: Honolulu, HI, USA, 2020; pp. 1–6.
41. Manchana, R. AI-Powered Observability: A Journey from Reactive to Proactive, Predictive, and Automated. *Int. J. Sci. Res. IJSR* **2024**, *13*, 1745–1755. [CrossRef]
42. Menken, I. *Virtualization Architecture, Adoption and Monetization of Virtualization Projects Using Best Practice Service Strategy, Service Design, Service Transition,... and Continual Service Improvement Processes*; Emereo Pty Ltd.: London, UK, 2008; ISBN 978-1-921523-49-6.
43. IBM. *IBM Process Reference Model for IT*; IBM: New York, NY, USA, 2008.
44. Eramo, R.; Said, B.; Oriol, M.; Bruneliere, H.; Morales, S. An architecture for model-based and intelligent automation in DevOps. *J. Syst. Softw.* **2024**, *217*, 112180. [CrossRef]
45. Cheng, Q.; Sahoo, D.; Saha, A.; Yang, W.; Liu, C.; Woo, G.; Singh, M.; Saverese, S.; Hoi, S.C.H. AI for IT Operations (AIOps) on Cloud Platforms: Reviews, Opportunities and Challenges. *arXiv* **2023**, arXiv:2304.04661.
46. Mell, P.M.; Grance, T. *The NIST Definition of Cloud Computing*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011; p. NIST SP 800-145.
47. Mulongo, N.Y. Key Performance Indicators of Artificial Intelligence For IT Operations (AIOPS). In Proceedings of the 2024 International Symposium on Networks, Computers and Communications (ISNCC), Washington, DC, USA, 22–25 October 2024; IEEE: Washington, DC, USA, 2024; pp. 1–8.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.