

# The Zero Repetition Bank Series

Transform IT Operations with Agentic  
AIOps for Resilience and Growth

March 2025



The better the question. The better the answer.  
The better the world works.



Shape the future  
with confidence

# Contents

## 01 Introduction

---

## 02 Strategic benefits of AAIOps for banks

---

## 03 Core components of AAIOps

---

## 04 Challenges in implementing AAIOps

---

## 05 The evolutionary path to AAIOps

---

## 06 Conclusion







# The Zero Repetition Bank

## Transform IT Operations with Agentic AIOps for Resilience and Growth

In today's fast-evolving banking landscape, IT operations are under constant pressure to balance resilience, regulatory compliance, and round-the-clock availability. Many banks are still caught in a cycle of firefighting, struggling to keep up with incidents and regulatory demands, while leaving little time for strategic growth. To break free from this reactive model, leading institutions are embracing a transformative solution: Agentic AIOps (AAIOps).

AAIOps transitions IT Operations from a reactive cost center to a strategic enabler.

### What is AAIOps?

AAIOps is more than just automated incident management—it represents an intelligent, self-governing IT ecosystem designed to detect, decide, and act autonomously. By integrating advanced AI with mature Infrastructure-as-Code (IaC) and Policy-as-Code (PaC) foundations, AAIOps evolves traditional IT operations into a proactive, adaptive powerhouse that minimizes human intervention while maximizing compliance, resilience, and efficiency. In essence, AAIOps transitions IT Operations from a reactive cost center to a strategic enabler.

### The journey to autonomy

Implementing AAIOps is a phased journey that starts with maturing IaC and PaC frameworks to ensure a compliant and consistent infrastructure baseline. Banks can then progress through stages of reactive automation, preventive analytics, and finally, full autonomy with AAIOps, where the system can self-heal, enforce compliance dynamically, and allocate resources intelligently. This journey is not only technical but cultural, requiring investment in skills, a shift in mindset, and a structured AI governance model to ensure transparency, accountability, and regulatory alignment.

### Strategic benefits

For banks, AAIOps offers transformative benefits:

- **Enhanced resilience:** Autonomous, self-healing capabilities prevent and resolve issues proactively, maintaining service continuity.
- **Compliance by design:** Continuous, real-time policy enforcement aligns IT actions with regulatory standards, providing a clear audit trail.
- **Optimized resources:** Cost-aware, AI-driven resource allocation reduces operational waste while meeting compliance requirements.
- **Reduced cognitive load:** With AAIOps handling routine tasks, IT teams are free to focus on high-impact, strategic projects.

### Key challenges and considerations

Implementing AAIOps is not without challenges. Legacy system integration, building trust with regulators, and managing cultural resistance require strategic program management. Establishing a governance framework with clear accountability, oversight, and audit capabilities is critical to ensure that AAIOps functions transparently and aligns with the bank's risk profile.

### Shape the future

For CTOs and CIOs, AAIOps offers a path to transform IT Operations from a support function into a strategic asset that drives resilience, innovation, and competitive advantage. This journey positions banks to meet the demands of tomorrow's digital and regulatory landscape, making IT Operations a key enabler of strategic growth and sustainability. Embracing AAIOps isn't just preparing for the future - it's shaping it.





1

Introduction to  
Agentic AIOps

# 1. Introduction to Agentic AIOps

## Key pointers

- AIOps automates monitoring and responses.
- AAIOPS independently analyses, decides, and acts.
- Agentic AI functions like a digital IT operations manager

---

Today's banking IT landscape is marked by an intense focus on incident response, data management, and regulatory compliance. Hybrid cloud environments and always-on demands lead to IT teams that are constantly firefighting, rarely having time to align operations with long-term strategy.

Where traditional AIOps automates some monitoring and responses, Agentic AIOps (AAIOPS) takes it a step further by introducing decision-making capabilities. Banks can leverage AAIOPS to build a strategic IT foundation that is not only reactive but also proactively autonomous, continuously working toward a state of Zero Repetition in processes and responses.

AAIOPS introduces an agentic capability—meaning it can independently analyze, decide, and act on operational issues in real time. This agentic capability involves more than simple automation. It's powered by collaborating sophisticated AI models that orchestrate complex tasks across IT environments, coordinating actions based on real-time data from multiple sources.

At its core, agentic AI functions like a digital IT operations manager. It orchestrates tasks while maintaining strict adherence to regulatory and security requirements.





2

Strategic benefits  
of AAIOPs for banks

## 2. Strategic benefits of AAIOps for banks

By embedding intelligence and compliance directly into operational processes, AAIOps creates a foundation that supports resilience, efficiency, and scalability, and delivers strategic advantages for modern banking IT.

### **Strategic focus and reduced cognitive load on IT teams**

With AAIOps handling operational and ensuring compliance, IT teams are freed from repetitive tasks and constant monitoring, reducing cognitive load and operational burnout. This strategic focus shift allows teams to concentrate on high-impact projects and innovations that align with the bank's long-term vision.

### **Enhanced operational resilience through autonomous self-healing**

AAIOps creates a resilient digital infrastructure. Its self-healing capabilities ensure that potential issues are addressed before they escalate, minimizing downtime and maintaining service continuity.

### **Optimized resource management and cost efficiency**

By embedding compliance, cost-awareness, and testing-driven decision-making into every resource allocation, AAIOps elevates resource management beyond simple automation.

### **Proactive, continuous compliance enforcement**

Compliance is built into every action AAIOps takes, from resource allocation to staging environment setup. This continuous compliance enforcement minimizes the risk of human error, reduces regulatory burdens, and provides a clear audit trail—vital in the highly regulated banking sector.

### **Reliable, compliant staging environments for testing and innovation**

AAIOps streamlines the setup and management of staging environments by leveraging preapproved IaC templates and PaC configurations. It provisions environments that meet both technical specifications and regulatory standards, adapting configurations as compliance requirements evolve.

### **Adaptive learning and continuous improvement**

AAIOps continuously learns from past actions, outcomes, and compliance requirements, refining its decision-making processes to become more effective over time. This adaptive learning capability allows AAIOps to stay aligned with new regulatory standards and operational insights, ensuring that the system evolves in tandem with both the bank's strategic goals and the regulatory landscape.





# 3

Core components  
of AAIOPs

### 3. Core components of AAIOps

#### Key pointers

- Banks can create a continuous improvement cycle for IT operations, improving efficiency significantly.
- IaC and PaC serve as the structural backbone of AAIOps.
- AAIOps builds on IaC and PaC by adding adaptability
  - without human intervention

To build an effective AAIOps framework, banks must adopt a foundational strategy based on two critical components from the Zero Repetition Bank's Continuous Improvement Cycle: Everything-as-Code (IaC and PaC), and Agentic AI capabilities.

#### Mature use of IaC and PaC

IaC and PaC serve as the structural backbone of AAIOps, enabling consistent, repeatable deployments across environments. With IaC, every aspect of infrastructure—from servers to network configurations—is defined in code, making it easily reproducible and minimizing the risk of configuration drift. PaC, meanwhile, embeds compliance into every layer of infrastructure, automatically enforcing regulatory policies and ensuring each deployment adheres to governance requirements from the outset.

Together, IaC and PaC provide a framework in which configurations and policies are standardized, governed, versioned, and auditable.

#### Leverage on Agentic AI capabilities

While IaC and PaC make infrastructure predictable and compliant, they are inherently static in nature. Changes to infrastructure or compliance standards generally require manual updates to the code or policy templates. This is where AAIOps adds a crucial layer of adaptability, allowing infrastructure to remain responsive to real-time demands and regulatory shifts without constant human intervention.

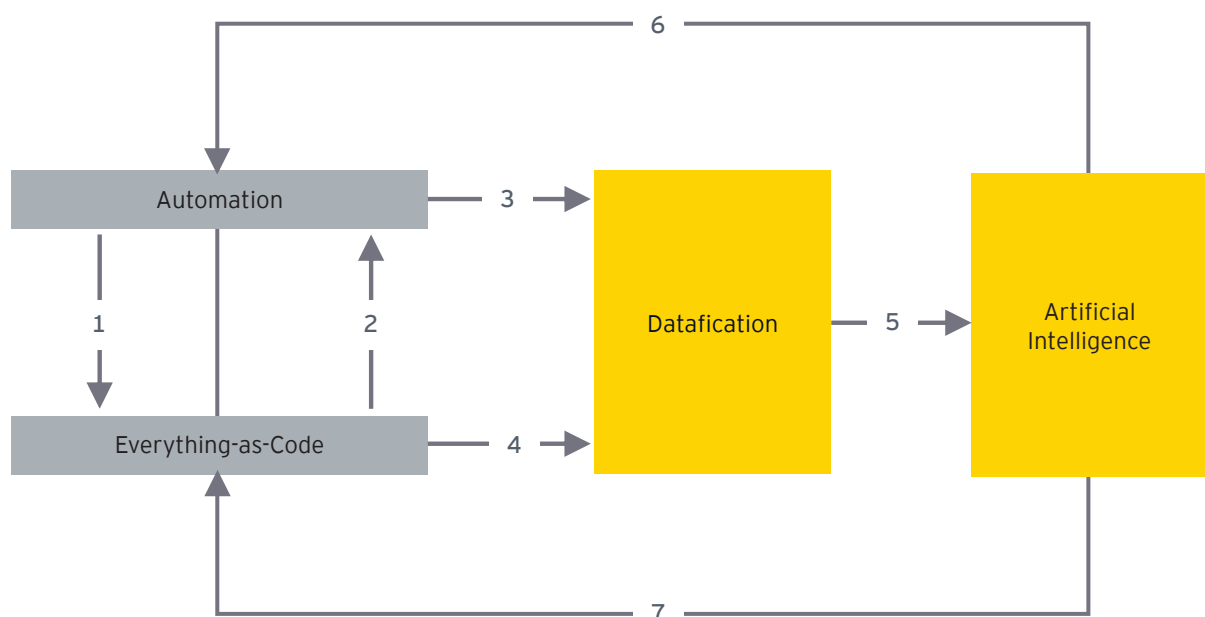


Figure 1: The Continuous Improvement Cycle



Unlike static policy enforcement, AAIOps delivers real-time compliance by dynamically adjusting IT operations to stay aligned with regulatory standards. For instance, if a new regulation impacts data handling, AAIOps can adjust configurations and apply compliance updates across infrastructure automatically, ensuring alignment without requiring template redeployment. This capability enables banks to respond rapidly to regulatory changes, minimizing compliance risk.

AAIOps isn't just reactive—it's proactive. By leveraging AI-driven analysis, AAIOps can forecast resource needs based on historical patterns and real-time data. This proactive capability allows it to allocate resources dynamically, responding to demand fluctuations or compliance updates in real time.

### **The Power of AAIOps**

Together, IaC and PaC establish a predictable, controlled infrastructure baseline, ensuring every deployment is compliant and consistent. AAIOps builds on this by adding adaptability, continuously responding to real-time operational demands and regulatory changes without human intervention.

### **Example: Providing compliant staging environments**

AAIOps can play a pivotal role in setting up staging environments by using preapproved Infrastructure-as-Code (IaC) templates and Policy-as-Code (PaC) configurations. Leveraging preapproved templates enables AAIOps to quickly provision compliant environments, ensuring each staging setup adheres to both technical specifications and regulatory standards from the outset.

With PaC, AAIOps can enforce compliance rules continuously across staging environments, adapting configurations if policies change. This role includes customizing environments based on specific testing needs, managing their lifecycle to keep configurations up-to-date, and providing full traceability for audits.

By automating these aspects, AAIOps ensures staging environments are reliable, compliant, and consistent indicators of production behavior, reducing repetitive setup tasks for IT teams.



gentic AT

4

Challenges in  
implementing AAIops



## 4. Challenges in implementing AAIOps

By addressing the specific challenges of implementing AAIOps, cultural, regulatory, and operational, with structured strategies, banks can build a solid AAIOps framework.

Despite its transformative potential, implementing AAIOps in a heavily regulated and risk-averse industry like banking comes with specific challenges. These obstacles aren't simply technical—they touch on cultural, regulatory, and operational aspects that banks must address for a successful rollout.

### Control and accountability

One of the core challenges with AAIOps is maintaining control and accountability within an autonomous system. When AI-driven operations take on decision-making roles, banks must ensure that every action and outcome can be traced, documented, and justified to meet regulatory standards. Establishing policies that require AAIOps to record and log every decision, along with the context and rationale, is essential for regulatory compliance and risk management.

### Balancing autonomy with human oversight

While AAIOps's autonomy is a powerful asset, banks need to establish boundaries for its decision-making. High-stakes decisions, such as those involving substantial financial risk or significant compliance impacts, will require human intervention. Identifying these thresholds and defining "stop points" where AAIOps actions pause for human review will help balance autonomy with accountability.

### Regulatory buy-in

In banking, regulators are often cautious about new technologies that remove human oversight, especially in decision-making processes. Autonomous systems like AAIOps could face scrutiny due to the perceived lack of direct human accountability. Banks will need to proactively work with regulators, demonstrating AAIOps's safety, control mechanisms, and auditing capabilities to build trust and secure approval.

### Integration with legacy systems and data challenges

Many banks rely on legacy systems with outdated data structures and integrations, making it challenging to seamlessly incorporate AAIOps. AAIOps relies on high-quality, real-time data to make informed decisions. In legacy systems, data can be fragmented, inconsistent, or poorly structured, impacting the accuracy of AAIOps processes. Banks need to invest in data normalization and integration layers to ensure that AAIOps has reliable data to work with, creating a foundation for accurate, effective decision-making.

By addressing these challenges with structured strategies, banks can build an AAIOps framework that improves operational efficiency while it aligns with the rigorous demands of the financial sector.



5

The evolutionary  
path to AAIops



# 5. The evolutionary path to AAIOps

Implementing AAIOps is not an overnight transformation but a phased journey that gradually evolves IT operations from basic automation to full autonomy. This path consists of several stages, each requiring a progressively higher degree of operational maturity, data governance, and AI capabilities. Banks can think of it in four main stages:

## 1. Maturing IaC and PaC: Building a predictable and compliant foundation

The initial phase focuses on establishing a stable and compliant infrastructure using Infrastructure-as-Code (IaC) and Policy-as-Code (PaC). By developing mature IaC and PaC practices, banks ensure that infrastructure configurations are reproducible, compliant, and fully governed. With IaC and PaC maturity, banks can confidently scale infrastructure while ensuring every component aligns with regulatory standards. This phase is essential for building the structure on which AAIOps can function effectively, as predictable configurations are key to enabling autonomous operations down the line.

## 2. Reactive AIOps: Automating incident monitoring

The first true AIOps phase focuses on moving IT operations beyond manual incident management by introducing basic automation. In this stage, banks leverage traditional AIOps capabilities to streamline monitoring, detection, and response to incidents, reducing reliance on human intervention for routine, repetitive tasks.

Reactive AIOps introduces rule-based automation and basic machine learning models that identify patterns in system behavior, allowing the system to detect anomalies and flag potential issues.

This phase reduces response times. It also establishes a feedback loop that captures data from incidents and responses, creating a base of historical data to support future predictive models.

## 3. Preventive AIOps: Proactively addressing potential issues with predictive models

In the third phase, AIOps evolves from a reactive approach to a preventive one. Banks start leveraging predictive models and data-driven insights to anticipate and address potential issues before they escalate, moving closer to a proactive IT environment.

Preventive AIOps uses advanced machine learning algorithms that analyze historical data to identify patterns and trends associated with past incidents. These algorithms enable the system to recognize early warning signs, triggering preventive actions such as reallocating resources, issuing preemptive alerts, or adjusting configurations. AAIOps also begins to apply PaC proactively, ensuring that compliance standards are upheld as it makes adjustments.

This stage significantly reduces the frequency and severity of incidents by anticipating and addressing risks early. Predictive capabilities lower the operational burden on IT teams, while proactive PaC enforcement ensures that regulatory compliance is maintained seamlessly. Preventive AIOps also improves resource utilization, as systems can anticipate and adjust for demand spikes and maintenance needs.



Figure 2: Four main stages to the evolutionary path to AAIOps

#### 4. AAIOps: Autonomous detection, decision-making, and strategic alignment

The final phase, full AAIOps, represents a shift from proactive management to autonomous operations. Here, AAIOps doesn't just respond or prevent—it independently detects issues, makes decisions, and takes actions that align IT operations with broader business strategies.

Agentic AIOps introduces agentic capabilities, where the system independently manages complex, interdependent tasks in real time. It combines advanced predictive analytics with self-healing, policy-driven compliance, and adaptive resource management to ensure that every decision and action aligns with both operational goals and regulatory standards. At this stage, AAIOps can autonomously create and test staging environments, initiate compliance-driven adjustments, and conduct outcome-based testing to confirm performance.

##### **An evolution from predictable foundations to strategic partner**

Each phase in the AAIOps journey requires a higher degree of operational maturity, data governance, and trust in AI-driven decision-making. Moving from Maturing IaC and PaC to Agentic AIOps transitions IT operations from predictable, compliant foundations to autonomous, strategic partners. With full autonomy, AAIOps becomes a self-governing, adaptable entity that anticipates needs, aligns with business goals, and ensures compliance, making it a cornerstone of modern banking strategy.

#### **Example: Compliance by AAIOps**

When regulatory standards evolve—such as new data residency mandates or encryption protocols—AAIOps doesn't simply enforce these updates. Instead, it autonomously initiates a suite of compliance and performance tests to validate the changes, ensuring that they meet both regulatory and operational standards without impacting system performance.

Following compliance updates, AAIOps reviews test results to determine whether the new configurations meet expected performance, security, and compliance thresholds. If issues arise—such as a degradation in performance due to enhanced encryption protocols—AAIOps can autonomously decide to roll back the change, adjust settings, or explore alternative compliance solutions. This informed, data-driven decision-making is key to balancing compliance with operational efficiency.

As AAIOps learns from each round of compliance testing and adaptation, it refines its decision-making for future updates. This continuous feedback loop enables AAIOps to anticipate the impact of similar changes in the future, reducing risks and enhancing compliance alignment.

This approach transforms compliance management into a proactive, adaptive process, where AAIOps not only enforces standards but also verifies and optimizes them through autonomous testing and decision-making. This intelligent compliance assurance gives IT teams confidence that infrastructure remains secure, compliant, and operationally efficient as standards evolve.



# 6

## Conclusion

## 6. Conclusion

The CIOs who dare to embrace the vision of AAIOps will future-proof their operations and position their IT operations departments as strategic powerhouses—autonomously resilient, agile, and aligned with evolving compliance landscapes.

AAIOps represents more than just an operational upgrade—it's a transformative shift that positions IT operations as a strategic asset in resilience, compliance, and innovation within banking.

As banking operations grow more complex and regulatory demands intensify, the value of a self-governing, adaptive ecosystem becomes undeniable. With AAIOps, banks can create an environment where IT operations do more than support—they lead, predict, and evolve in alignment with broader business goals.

The path to full AAIOps autonomy is a phased journey that begins with maturing IaC and PaC, establishing a compliant, predictable foundation upon which AAIOps can operate. Moving through stages of reactive automation, preventive intelligence, and ultimately agentic decision-making, AAIOps gradually transforms IT Operations from a reactive support function into a proactive, strategic asset. This journey isn't just about technological progression; it's primarily a cultural shift,

requiring a commitment to upskilling, governance, and adaptability across all levels of the organization.

For CTOs and CIOs, the path to AAIOps may seem daunting, with unique challenges in governance, legacy integration, and cultural alignment. Yet the rewards are profound. Those who dare to embrace this vision will future-proof their operations and position their IT operations departments as strategic powerhouses—autonomously resilient, agile, and aligned with evolving compliance landscapes.

In an industry where resilience and compliance are paramount, AAIOps offers a powerful advantage, enabling banks to innovate, scale, and thrive. The future of banking IT belongs to those who are willing to take this leap toward autonomy, transforming operations into a cornerstone of competitive advantage.

### **Don't wait for the future—create it with AAIOps.**

Now is the time to act. Embrace the journey to AAIOps and lead your bank into a new era of innovation and resilience. Start by evaluating your current IT operations, identifying areas for automation and predictive intelligence, and investing in the necessary upskilling and governance frameworks. The transformation won't happen overnight, but with a clear vision and commitment, you can position your IT operations as the strategic asset for your bank. Don't wait for the future—create it with AAIOps.



# Meet our Technology Strategy & Transformation team

---



**Remi Hesterman**  
Partner  
EY Netherlands  
E: [remi.hesterman@nl.ey.com](mailto:remi.hesterman@nl.ey.com)



**Martin Borman**  
Strategic Solutions Architect  
External advisor to EY  
E: [martin.borman@nl.ey.com](mailto:martin.borman@nl.ey.com)



**Matthieu Griffioen**  
Director  
EY Netherlands  
E: [matthieu.griffioen@nl.ey.com](mailto:matthieu.griffioen@nl.ey.com)



**Sven Schenkel**  
Director  
EY Netherlands  
E: [sven.schenkel@nl.ey.com](mailto:sven.schenkel@nl.ey.com)

## EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

### All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

© 2025 EY Nederland B.V.  
All Rights Reserved.

ED NONE

[ey.com](https://ey.com)