A whitepaper of

AIOps: A practical framework for AI driven operations in the telecom industry

Objective(s): To identify the gaps between traditional and AI-driven operations and establish a practical framework for redesigned and re-engineered processes to enable AI operations (AIOps).

Contributing companies and co-editors/contributors

TM Forum, Aaron Boasman-Patel (Editor)
Huawei, Luca Franco Varvello (Contributor & Co-editor)
China Telecom, Zhang Ke
Orange, Tayeb Ben Meriem
Orange, Sophie Nachman
Huawei, Wang Lei
Huawei,-Wangmingxue
Huawei, Sarah Haojing
HKT, Yue Chiu-Chung
HKT, Derek Chen
BolgiaTen, Professor Paul Morrissey
Intracom Telecom, Nikos Anastopoulos
TIM, Massimo Banzi

First Release

July 2020

Contents

Executive summary

Artificial Intelligence (AI) is going to have a profound effect on communication services providers (CSPs) and it will transform their networks, IT and service operations; enabling them to deliver new complex services across the digital ecosystem. AI will allow service providers to add the agility, speed of service delivery, reliability as well as deliver the significant cost-savings needed to compete, co-exist and even partner with over-the-top (OTT), hyperscalers, and new nimble digital players.

It is estimated by the McKinsey Global Institute[1] that AI could contribute an additional 1.2 percent to annual GDP growth for at least the next decade, which accounts to over USD $13 trillion of economic activity by 2030. This coupled with Bain's prediction that 5G could be worth over $400 billion to CSPs[2] in the B2B2x marketplace, operators will be well placed to exponentially grow their revenues which hasn't been seen since the early 2000s. New business models enabled by 5G and AI are not the only key drivers for cognitive and autonomous network deployment. The World Economic Forum[3] have estimated that AI could save CSPs a massive $46 billion in customer acquisition costs and lost revenue through network performance and a 30% reduction in mobile infrastructure spending by using AI for better network planning.

Aside from the economic benefits, technological advancements outside of AI are making its deployment a must. The advent of new wireless technologies such as 5G have the potential to add even more complexity to the network, particularly in radio access network operations. 5G will make RAN more complex as it needs forests of tiny antennas to exploit the very high frequency bands (mm Waves) it will run on. In addition, it is estimated by 2025 that there will be a total of 100 billion device connections[4] around the world, which will put a huge amount of pressure on networks. More devices equals more data that run across an operators' network and IDC forecasts that by 2025, data will grow by ten times and reach 163 zettabytes (a trillion gigabytes).

As the number of devices and the internet of things (IoT) grows, network and service management must be zero-touch as it is not feasible for manual processes to support the volume and velocity of changes that must happen across the network. A network servicing 10 million endpoints and 10,000 nodes could see these numbers increase by up to five times, which in terms of incidents per hour could lead to a 25-times increase from 400 incidents to as many as 10,000 per hour[5]. This is impossible to handle manually, and that is why services providers need to deploy AI and automation in their networks.

Large-scale deployments of AI in operators' networks creates huge operational challenges such as how to govern, deploy, operate, control and maintain hundreds or thousands of AI models and components which will eventually form part of their core IT and network systems architecture. Unlike the traditional software, AI software learns and evolves autonomously when exposed to new input data. Unlike traditional software, AI models are "black boxes" which are potentially even more fragile; exposed to bias and are nondeterministic by nature. In order to address these challenges, TM Forum and its members are leading an industry initiative called "AIOps Service Management" and are creating an industry agreed framework focused on reengineering the multiple processes of the software lifecycle and service operations management to handle and govern AI software at scale. This will enable operations teams, process owners and business users to exploit AI safely and properly maximizing its benefits, mitigating risks, and ensuring the appropriate level of network and service quality.

The AIOps Service Management Framework is applicable to any type of architecture due to its agnostic design and can operate as an independent process framework and will help service providers manage the deployment of AI into their current and target state architectures. The AIOps Service Management Framework is, however, part of TM Forum's Open Digital Framework (ODF), which includes the target Open Digital Architecture (ODA). The ODA is an open, modern, software-based technology architecture that enables new operating and business models fit for the 5G era. It is loosely coupled, cloud-native, data and AI-driven; made up of standard components which can be easily procured and deployed, without the need for customization. More information about the Open Digital Architecture can be found here[6], including the latest whitepaper which sets out an industry agreed vision of the software market and services delivered through an open digital architecture.

---

[1] https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy

[2] Source: Bain, https://www.bain.com/insights/telcos-400-billion-as-a-service-enterprise-gold-mine/

[3] Source: http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-telecommunications-industry-white-paper.pdf

[4] https://www.huawei.com/minisite/giv/Files/whitepaper_en_2018.pdf

[5] http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-telecommunications-industry-white-paper.pdf

[6] https://www.tmforum.org/oda/

Why we need a new approach to IT & network operations processes

Artificial Intelligence (AI), combined with and enhanced by advanced analytics, big data and virtualized computing power, will drive the automation and enhancement of CSPs' network, IT service and business operations. AI capabilities will gradually be infused in IT, network, and business systems and services through the implementation and deployment of AI models and components in all layers of CSPs' architecture.

Systems running in IT & network operations will be providing AI capabilities through embedded AI models and AI components. They will improve various business and operational processes including; Business and Operations Support Systems (BSS & OSS), data analytics, enterprise resource planning (ERP), 3rd party and digital applications.

AI deployments will bring tremendous opportunity to improve the business processes, business services and the CSPs' overall performance but it will also create some challenges. One of the main challenges for CSPs operations will be how to govern, deploy, operate, control and maintain hundreds or even thousands of AI model instances within their IT and network systems architecture. Unlike traditional software, AI software (i.e. any software embedded with AI technology) may reason, learn and evolve autonomously when exposed to new input data and in addition AI models tend to be "black-boxes" which are potentially even more fragile, exposed to bias, and are nondeterministic by nature.

In order to address these challenges, traditional service management processes need to be revisited and adapted to enable operations teams, process owners, and business users to exploit AI safely and correctly. This will allow CSPs to maximize the benefits of their AI deployments, mitigate risks and ensure the appropriate level of service quality.

Managing traditional software operations with hundreds or thousands of applications requires the setup of solid and repeatable service management and governance processes. This ensures that the quality, reliability and compliance of the service operations can be met. These robust, appropriate and reliable service management processes become even more important when CSPs move away from a gradual introduction of AI in their operations to large scale deployments, where the need to control the dynamic and autonomous AI software and its impacts on the business and internal services become greater.

Before scaling AI, CSPs must perform a deep assessment and gap analysis of their current IT and network service management processes, in order to understand which processes need to be redesigned and the actions taken in order to transform their operations. This will enable them to be ready and robust enough to support large-scale AI deployments. To help service providers achieve this, TM Forum and its members are leading an industry initiative called "AIOps Service Management" and are creating an industry agreed framework focusing on reengineering the multiple processes of the software lifecycle and service operations management to handle and govern AI. Every AIOps process described across the lifecycle will address, the "as-is" process, provide a gap analysis, along with AIOps process reengineering guidelines and use cases.

The starting point of the evolutionary journey towards AIOps is the 'AS IS', where existing practices like ITIL, Agile and DevOps are partially or fully adopted. From this perspective, AIOps Service Management as an evolution or a complement of existing frameworks (DevOps, Agile, ITIL ...), where we add and suggest specific principles and practices that need to be adopted and implemented for managing a blend of AI and traditional applications in complex operations environments (Figure 1). AIOps Service Management is based on existing well-established practices. We believe that ITIL, Agile and DevOps are necessary pre-requisites to manage AI effectively.

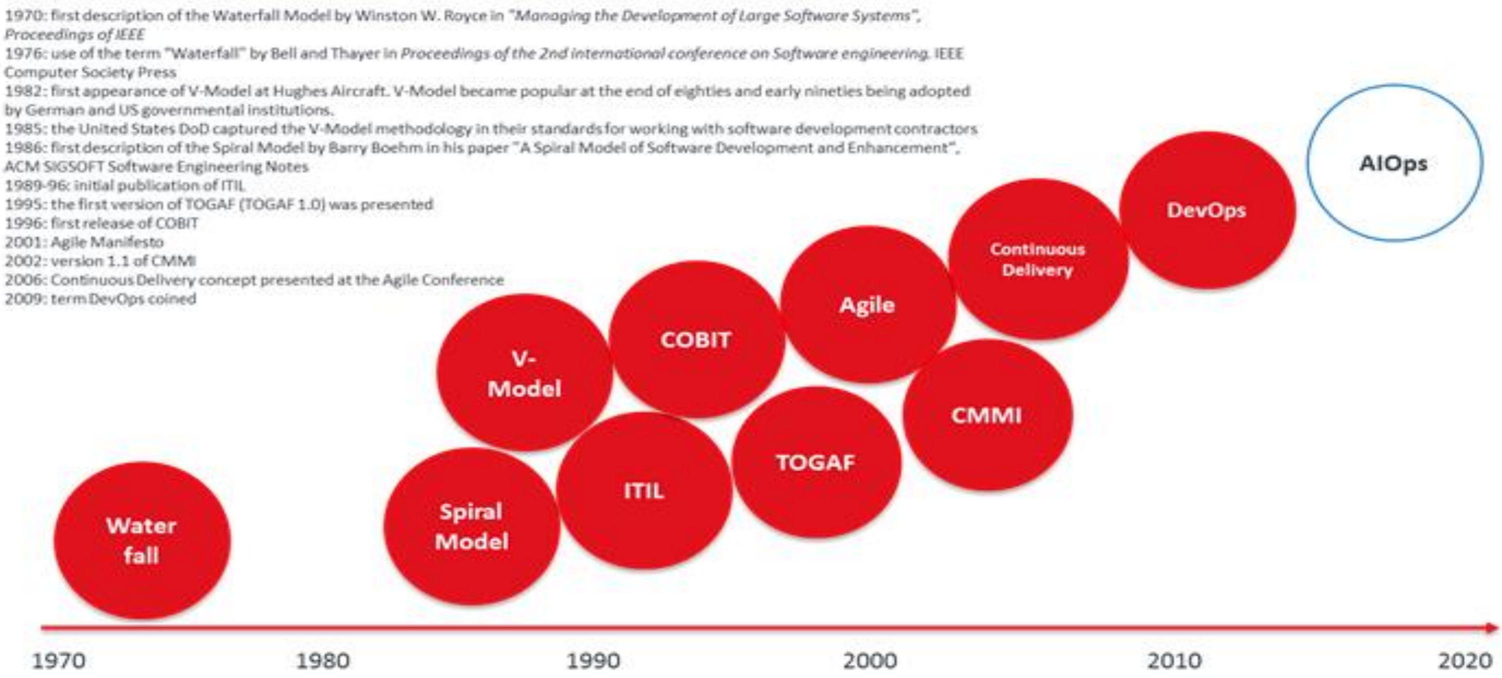

Figure 1. Main Software Engineering & Operations Management Practices

AIOps in the software lifecycle

In order to understand the multiple processes that need to be redesigned across the software lifecycle to enable AIOps we first need to consider the general software lifecycle model as shown below (figure 2).

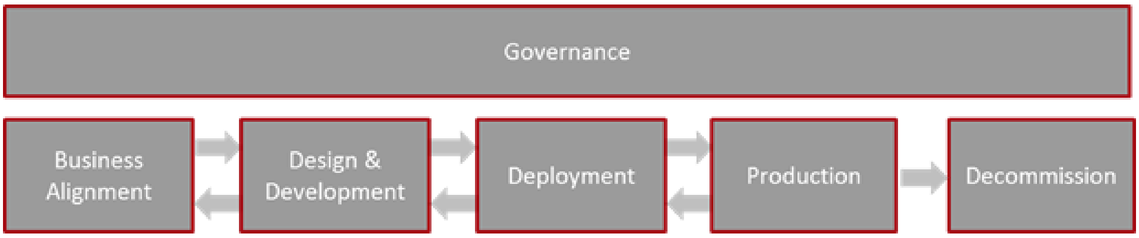

Figure 2. General Software Lifecycle

The AIOps Service Management Framework is agnostic to any specific software management methodology and is general enough to be inclusive of the building blocks of most software engineering lifecycles, including traditional (like waterfall or V-Model) and Agile practices. Most software and solutions lifecycles include the following steps or phases, even if they have different names or approaches:

- **Business Alignment**, which includes the understanding of business requirements and the corresponding formal and detailed specifications and/or prototyping.
- **Design & Development,** which covers functional and technical specifications, solution architecture, coding, configuration, testing stages (unit testing, system testing etc.). For AI/ML software, this step also includes the ML training of AI models, which does not exist for traditional software.
- **Deployment**, also called transition or commit in some contexts, representing the bridge or gate between the Development and Production stages.
- **Production**, the subset of processes aimed to operate and maintain the services in Production live environments.
- **Decommission**, addressing the removal of a system release from Production.
- **Governance**, which includes, among other processes, Strategy Management, Quality Management, Risk Management, Security Management, Compliance Management etc. In AIOps, it shall address new practices such as “Bias Management” that may be necessary to govern sensitive or fragile AI models exposed to bias. We refer in this paper to Operations Governance as the subset of governance processes that are needed to manage and govern specifically the Deployment and Production stages of the lifecycle.

The scope of the work TM Forum and its members are undertaking will focus on reengineering operational processes for AIOps in the following process areas:

- Deployment
- Production
- Decommission
- Operations Governance

Addressing the gaps between traditional and AI software to successfully enable AI-driven operations

AI is a type of software-based technology, yet there are significant differences between traditional and AI software. The specific characteristics of AI software creates the challenge of managing, governing and operating systems and processes differently. These challenges mean that we need to identify the current operational and process gaps between traditional and AI-driven operations and redesign those processes so AI can be deployed and managed safely.

From an operations management perspective we have identified the following main differences between traditional and AI software, without the pretension to be exhaustive and comprehensive:

1. The software lifecycle for traditional systems is mainly driven from left to right, i.e. from Development to Operations. In AIOps a new, critical aspect to manage is the self-driven software updates in Production that generate a new flow from right to left, i.e. from Operations to Development, which does not exist for traditional software. Current continuous improvement practices are based on human feedback and interventions, not on software-driven updates. In AI-operations the lifecycle of AI components is bidirectional as they can also flow from Operations back to Development. This is because AI models may autonomously change their state and configuration in Production (online learning, self-driven updates …) without human intervention which requires a prompt and comprehensive retrospective evaluation (Figure 3).

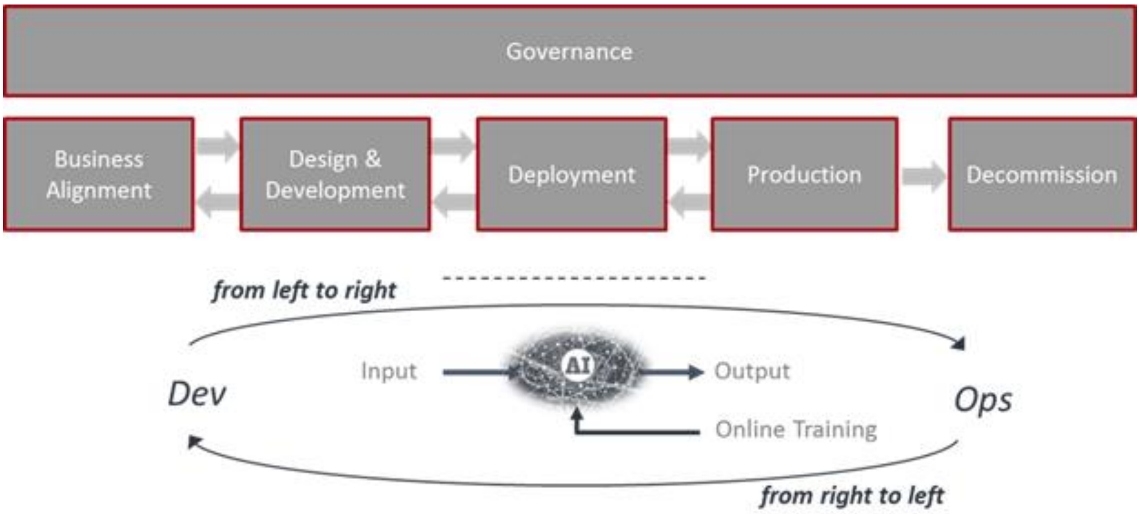

Figure 3. AIOps: from Dev to Ops and from Ops to Dev

2. All software evolves. Continuous Improvement, Lean and Kaizen principles have been extensively adopted in software engineering and service operations management. The retrospective approach and principles which are part of Agile and DevOps methodologies must also be applied in AIOPs. For traditional software, evolution and maintenance is planned or can be planned, however, for AI software, the evolution is both planned, spontaneous, autonomous, and self-driven at the same time as it is powered by the embedded AI engine.

3. Before the introduction of AI, Production environments have always been viewed as static, locked down and sterile environments where all changes go through a planned change management process. Agile and DevOps practices have accelerated and streamlined the preliminary processes leading up to Production (development and testing process, integration and deployment process) but the core static essence of Production environments have not significantly changed. The introduction of AI models in operations challenges this traditional static view and transforms the Production environment to be intrinsically dynamic. AI software is changing the operations management approach and the operations culture, which will need to govern dynamic live environments, overcome the "fear of change" and manage consequently the risks associated to the dynamic changes in Production.

4. In traditional software engineering, the baseline and the starting point from where we develop new software are usually well known. With the introduction of AI, the baseline of the software become unclear as it is always dynamically changing.

5. Data has a vital role and is one of the key components of the structure of AI models. It is the fuel driving the evolution of AI systems. New input datasets enable the evolution of AI models which can bring new and different outcomes. For these reasons in AIOps, data operations become even more critical and central (AIDataOps).

6. Machine Learning (ML) training of AI algorithms and the re-training of AI models in Production are brand new processes in software development and operations management, which do not exist in traditional software lifecycles.

7. AI models are nondeterministic by nature. All software in large and complex operations can be considered at a certain degree nondeterministic because of the high number of involved variables and unpredictable scenarios that they may face. However, traditional software is or should be deterministic by definition, i.e. given the same input it provides the same output. AI models are different as they may behave differently in the same circumstances because their internal state and internal logic may permanently change and evolve.

8. AI software can be even more fragile than traditional software. As for any software, a small difference between versions of code, software configurations or between environments baseline can create issues, defects or unexpected outcomes. AI software is even more fragile as a new byte (unit of digital information) in the input data can destabilize the AI model.

9. AI models are exposed to the additional risk of bias. AI software can be biased with inappropriate, incomplete, corrupted, incorrect or fraudulent input data. They are also susceptible to the same existing weaknesses for traditional software such as viruses, malicious agents, sabotage, vulnerabilities etc.

10. AI models are mostly "black boxes" which makes it challenging to determine why AI models make a specific decision, prediction, or classification. There are hidden dependencies inside the models, resulting from the combination of the integration of input data, training parameters, configuration settings etc. The internal logic of the code moves from the code itself to the "intelligence" embedded in it. While code review of software and other audit techniques would usually clarify the overall logic behind the behavior of traditional software, for AI software this would not be sufficient. Additional and different approaches and techniques are needed to increase the transparency and the "explainability" of AI software.

11. Continuous Delivery and DevOps practices have taught us that software should be considered as being in a permanent working state or beta state. This principle is even truer for AI models, which are pieces of software with the capability to learn spontaneously and continuously when exposed to new data. By definition, AI models are in a permanent evolutionary and working state (like human brains...).

12. The intrinsic characteristics of the AI models (listed above) amplify further the management responsibility of the Operations departments, making them even more central and accountable for the service quality, service performance, and for the proper and timely control and maintenance of the continuously evolving and non-deterministic AI systems in Production.

13. With the deployment of AI at scale, Production environments become dynamic by nature. Deploying only offline AI modules would certainly create new challenges but the complexity of its operation would be limited. To leverage the full potential of AI, CSPs need to learn how to manage both offline and online AI models in Production, supervising their continuous dynamic evolution and ensuring the full control and governance of operations.

Traditional Software	AI Software
• Software lifecycle is driven from left to right, from Dev to Ops • Evolution is planned • Production environments are static and locked down • Changes go through a planned Change Management Process • Baselines of software are usually well known • Deterministic • Easily auditable • Fragile	• Online learning, generate a new flow from right to left, from Ops to Dev • Evolution is both planned and autonomous/self-driven • Production environments become dynamic, constantly changing • Base lines of software become blurred • Nondeterministic • Black boxes • Even more fragile than traditional software and exposed to bias and corrupted knowledge • ML training and retraining of AI models are brand new processes in the software lifecycle • Operations (including data ops) become even more central than today

Figure 4. Main differences between traditional software and AI software

AIOps Service Management Framework

Due to the differences and gaps between traditional and AI software, we must rethink and redesign the service management processes to prepare them to manage, govern and safely operate AI systems. In addition, we need to enact processes that enable a blend of AI and traditional applications to run together simultaneously in CSPs' IT and Network operations.

The AIOps Service Management Framework addresses the technical and operational processes needed to deploy and integrate significant numbers of AI components and their relevant business capabilities into existing CSPs' IT and Network operations.

Deploying the framework will enable you to:

- Redesign the Deployment processes to release and commit AI software and their components to Production.
- Redesign the Production processes to operate and maintain AI-based systems.
- Redesign the Operations Governance processes to govern AI-based systems.
- Deal with fast flows of changes coming from Dev to Ops and from Ops to Dev for both offline and online models.
- Integrate effective AI data operations and ML training practices in the AI software operations management.

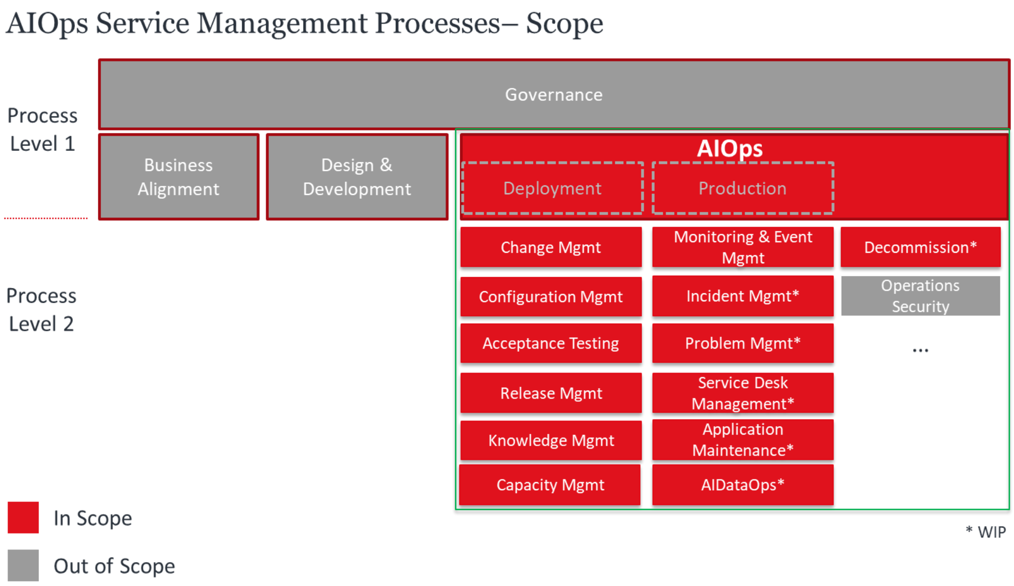

Figure 5. Lifecycle stages in scope of the AIOps work stream

The strict segregation between Deployment and Production processes that are typical in traditional operations are no longer valid in AIOps as the processes become blurred and indistinguishable. This is due to the dynamic nature of AI software and its capability to learn and evolve autonomously, which creates a continuum between the Deployment and Production stages. AI components move permanently from the deployable state to the live state and vice versa, which challenge the distinguishable frontiers existing today between Deployment and Production. For this reason, we consider the Deployment and Production processes as part of AIOps and we do not assign them to any specific stage of the lifecycle. This will give companies greater agility in their IT operations, as they can organize their processes in stages and assign responsibilities to the teams according to their strategy, organizational choices, and operational context.

The table below shows the processes that are currently in development as part of the AIOps Service Management Framework. We acknowledge that Operations Security is a key vital process in any good operations management framework, however, it is not in scope of this work. Information and Infrastructure security needs to be addressed and treated as a whole and comprehensive discipline that crosses all other domains and all stages of the lifecycle (from Design to Decommission including Governance) and that is pervasive in strategic, operational and cultural levels.

Process	Brief Description
Configuration Management[7]	Configuration Management ensures that all components (also called Configuration Items, CIs) of systems and services are uniquely identified, baselined and maintained and that changes to them are controlled across the whole service lifecycle.
Change Management[8]	Change Management ensures a smooth transition of all changes to Production live environments. It minimizes the risks, preserves the quality of service, avoiding incidents and outage, and prepares the final users/consumers to adopt the new capabilities/features.
Acceptance Testing[9]	Acceptance Testing ensures the overall quality against the expected targets of all new and existing updated software and services, before declaring and certifying them as "operations ready" and "deployable" to the Production live environment.
Release Management[10]	Release Management plans and manages the deployment of any software release from Development to Production environments (and in general, to any relevant environment).
Knowledge Management[11]	Knowledge Management ensures that reliable and complete information and knowledge is available to the right parties (people, consumers, 3rd parties...) at the right time throughout the service lifecycle.
Monitoring & Event Management[12]	Monitoring & Event Management, monitors, detects, filters, and correlates all relevant events occurring throughout the Production environments and initiates the corresponding activities to respond to and address those events, when necessary and appropriate.
Incident Management	Incident Management addresses all events that have or could have relevant impacts (outages, incidents, defects/bugs, operational issues, quality degradation ...) on the services and, in line with their priority, manages the recovery of the service operations according to the agreed SLAs, minimizing the impacts on users and business processes and managing the necessary communication.
Problem Management	Problem Management is responsible for the diagnosis of the root cause of incidents, issues, vulnerabilities, and weaknesses related to systems and services, and, in line with their priority, ensures the permanent resolution of those problems, when appropriate.
Service Desk Management	Service Desk Management is the process responsible for managing the lifecycle of all different types of demands (Service or User Requests) submitted by the end-users to the Service Desk.
Application Maintenance (Preventive and Perfective Maintenance)	Application Maintenance ensures the proper modifications of software and its components after delivery to Production in order to improve their performance, quality, efficiency, or other relevant attributes.
Capacity Management	Capacity Management ensures that cost-justifiable capacity of services and related components (software, hardware, network etc.) is able to deliver, the agreed service level targets, presently and in the future, in a timely and effective manner in the specific context of the CSP.
AIDataOps	Data Management is a key practice to ensure the data availability, accessibility, security, compliancy, and at the same time the systems efficiency and performance. Being data the fuel driving the operations and evolution of AI software, AI Data Operations management (AIDataOps) become vital to ensure that the right data in Production are properly collected, processed, transformed, stored, safeguarded, available and accessible at the right time, according to the business needs, laws, regulations, security policies and efficiency drivers.

Figure 6: Table showing processes that are currently under assessment as part of the AIOps Service Management Framework

[7] https://www.tmforum.org/resources/how-to-guide/ig1190a-aiops-configuration-management-v3-0-0/
[8] https://www.tmforum.org/resources/how-to-guide/ig1190b-aiops-change-management-v1-0-0/
[9] https://www.tmforum.org/resources/how-to-guide/ig1190d-aiops-acceptance-testing-v1-0-0/
[10] https://www.tmforum.org/resources/how-to-guide/ig1190c-aiops-release-management-v1-0-0/
[11] https://www.tmforum.org/resources/how-to-guide/ig1190e-aiops-knowledge-management-v1-0-0/
[12] https://www.tmforum.org/resources/how-to-guide/ig1190f-aiops-monitoring-and-event-management-v1-0-0/

Understanding the implications of AIOPs

AIOps is going to have far reaching implications across CSPs organizations, not only in terms of changes needed to redesign traditional operational processes, but also in the way that AI-enabled systems are monitored, controlled, governed and procured. AIOps is going to affect the entire software lifecycle and CSPs need to be able to quickly adapt to these changes to ensure they can be deployed and managed safely and effectively at scale. In addition to this, AIOps is going to force CSPs to rethink the management and organization of their businesses and the roles and skillsets needed. This is because AIOps is a discipline which is outside of the normal operational practices of service providers and does not have the traditional operational boarders between teams. Instead, AIOps transits across several departments and therefore questions of ownership and lines of responsibility begin to emerge which need to be addressed. AIOps by nature forces different teams across the organization to work together to achieve common operational goals.

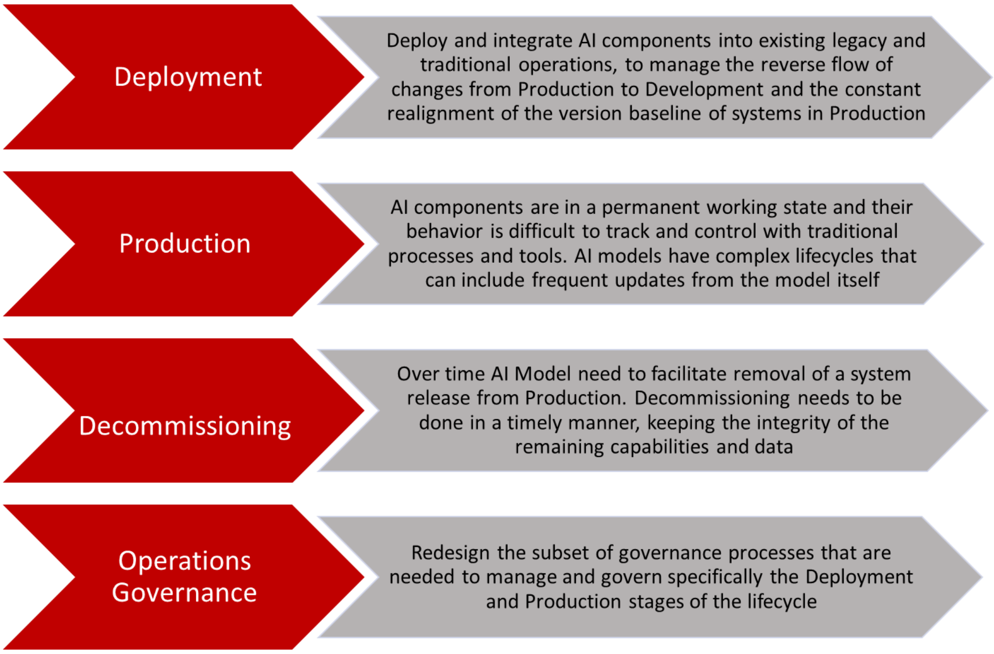

Figure 7: Showing the challenges of AIOps through the in-scope lifecycle stages

The strict segregation in traditional operations between the Deployment and Production stages become blurred in AIOps, challenging the distinguishable frontiers existing today between Deployment and Production. For this reason, we consider that the traditionally siloed Deployment and Production stages and organizational units shall be redesigned in order to create a convergent and merged process as area able to manage the dynamic nature of AI components.

The end goal of the transformation journey is to reengineer the Deployment, Production and Governance processes. A new solid AIOps Service Management layer will be created (figure 8), which will be the core and the barycenter of the service, applications and infrastructure management. This will ensure the effective, efficient and safe support of AI-driven business processes. AIOps causes the operations departments to play a strategic and central role for the service and business performance as they need to manage and govern the autonomous and self-driven evolution of the AI components albeit ensuring the expected outcome of the overall service quality.

As part of the transformation journey, the operations teams need to be reorganized in order to define clear roles and responsibilities on the AIOps Service Management layer and the organizations will need to develop and incorporate the proper skills and resources to handle the new types of AI-based applications. Every company will need to reorganize their teams and assign responsibilities to them according to their strategy, organizational choices and operational context.

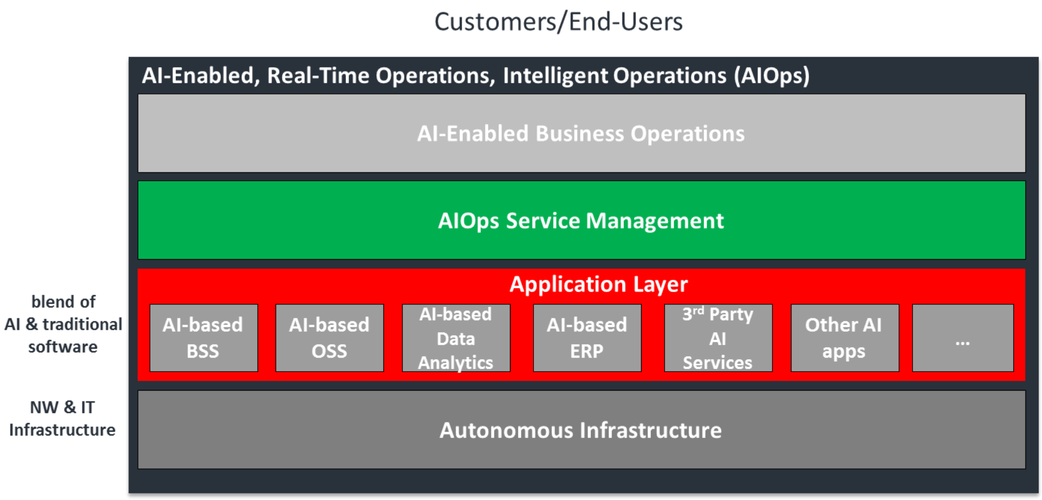

Figure 8: AI enabled operations framework

Early deployments of AIOps by CSPs has mainly been taking place in the Service Operation Centre (SOC), so it serves as a good use case to look at how future teams could be structured with their roles and responsibilities. The SOC is a place where a dedicated team of AIOps individuals can be assigned to look at service management issues which are utilizing AI models in their day-to-day operations.
In one of the AIOps use cases analyzed in the workstream activities, the team of AIOps engineers has be structured in the following way:

- **Policy Design Engineer**, who is responsible for requirement analysis, operations and orchestration design
- **Data Analysis Engineer**, who is responsible for identifying AI opportunities, AI application design, data modelling etc.
- **Orchestration Engineer**, who is responsible for designing user test cases, coding & testing, acceptance testing, install to runtime, post-implementation monitoring etc.

In the first instance, the team would concentrate on managing the AI Model associated with service management, e.g. production processes, monitoring and event management, incident management, problem management, capacity management etc.

As the proliferation of AI models develop across the organization, the team can be given the mandate to oversee other AI operational model domains such as customer service, revenue management, finance, revenue assurance etc. In traditional DevOps and DevSecOps, we are now seeing full stack developers (multi-faceted approach), but in the AIOps environment, full stack enabled individuals are quite a way off, so breaking down the roles and responsibilities as outlined above is the most sensible solution in initial deployments.

We have shown an example of the organizational changes needed in the SOC, but for large-scale AIOps deployments to be successful, more fundamental structural changes to the entire organization need to be made. The new operational environment under the development and data arm of the organization within an Open Digital Architecture Environment (ODA) needs fundamental adjustments to existing organizational structures. AI will bring new challenges to the organization which are not capable of being addressed through existing, traditional structures. The final organizational structure will evolve dynamically as AI and ODA capabilities evolve and mature, but we need to make incremental changes now to ensure we can manage AI modules dynamically, at speed of the customer and at scale.

The implications of AIOps go far beyond people and processes. Another challenge of AIOps is the number of systems and tools supporting the service operations management. There is a plethora of tools and platforms available in the market supporting the IT and Network operations (monitoring platforms, incident management and trouble ticketing tools, configuration and version management systems, testing platforms, knowledge management tools etc.). These tools will also evolve and be adapted to manage and operate AI-based systems and their components. Our analysis is tool-agnostic, however, the process guidelines and principles stated and recommended in our AIOps Service Management framework should be taken as input and requirements for the redesign and transformation of all underpinning service management tools, This will generate new families of tools that are prepared to support both traditional and AI software. More information about the TM Forum's AI, Data and Analytics work can be found here: https://www.tmforum.org/ai-data-analytics/