07-11-2023

White Paper:
OAV Maturity Model

Abstract

The Orchestration, Automation and Virtualisation (OAV) maturity model presented in this document has been created by the Network Development Work Package (WP6) of the GN5-1 project to provide a tool to compare and recognise similar goals and needs across NRENs, thereby boosting collaboration and cooperation in OAV in the research and education space. The maturity model enables organisations to assess their OAV capabilities, described through a set of dimensions. The results of the maturity model survey can help organisations evaluate their current state and determine their objectives in terms of OAV evolution, as well as establish a roadmap to follow in order to increase their OAV maturity level.

Table of Contents

Table of Figures

Executive Summary

Orchestration, Automation and Virtualisation (OAV) are vital to the successful digital transformation of any organisation, as they enable the possibility of offering self-service provisioning and on-demand services. Identifying their current capabilities, strengths, weaknesses, threats and opportunities is key if R&E organisations are to succeed and reach an optimal status in these areas. The OAV Maturity Model (OAV MM) designed by the Network Development Work Package (WP6) of the GN5-1 project aims to aid organisations in their journey towards digital transformation and full implementation of OAV.

The model defines four primary dimensions that describe various aspects of OAV (Architecture and Technology, Processes and Services, Vision and Strategy and People and Organisation), with each dimension further specifying sub-dimensions that emphasise the most significant OAV domains within it. Six maturity stages are used to characterise the level of OAV adoption and management by organisations, ranging from no OAV adoption to cutting-edge OAV implementations:

0. None (sit) – Organisations at this stage have either not implemented OAV in their production networks or have implemented minimal virtualisation.
1. Ad Hoc (crawl) – OAV has gained traction, and engineers and development teams are interested.
2. Reactive (walk) – OAV is now part of the strategic decisions of upper management and the initial pilot use cases (on a service or process level) are being implemented in production;
3. Integrated (run) – The company has now transitioned to an OAV architecture.;
4. Proactive (fly) – The organisation is upgrading to an advanced multi-domain OAV platform for all services, aiming to achieve proactive behaviour in all aspects of its activities and to be ready to join a partner's ecosystem.
5. Self-* (energise) – The organisation is exhibiting self-anything behaviour. New components, functionalities, partners, and services are automatically discovered, and interoperability is achieved in a seamless manner.

Based on their responses to the OAV MM, organisations are issued with a report highlighting their stage of progress and possible actions to take in each of the areas considered, and are assigned an overall maturity level. The survey can be repeated on a regular basis to help organisations track their OAV evolution.

The OAV Maturity Model is one of the resources offered by the Network eAcademy in GN5-1 WP6 to support organisations in their human capital development and digital transformation.

1 Introduction

Comparing and benchmarking levels of orchestration, automation and virtualisation (OAV) across different organisations in the research and education community presents a challenge. Previous research has shown that there are significant differences between surveyed NRENs in the GÉANT community [D6.2-GN4-3] in terms of user groups and use cases, implementation approaches, maturity levels, tools, systems, processes etc. Thus, a maturity model was needed that could be applied regardless of the type of institution.

The first step towards this involved an exploration of existing maturity models (see References: Maturity Model 1, Maturity Model 2, Solar, M., Sabattin and J., & Parada, V. (2013), Bass, J. M. (2011), Haris, F. (2010), Pham, Q. T. (2017), De Sousa Pereira, R. F., & Da Silva, M. M. (2010), Rathfelder, C., & Groenda, H. (2008), Net, T. (1998)) and their applicability to the R&E community. From the results of this analysis, it became evident that existing maturity models did not adequately align with the specific OAV needs and dimensions of the community. Therefore, an OAV maturity model was created following specific guidelines [Proenca, D. (2016)], encompassing four dimensions: **Architecture & Technology, Processes & Services, Vision & Strategy, and People & Organisation.** Each dimension in turn consists of different sub-dimensions. For each sub-dimension, six distinct stages can be considered, which have also been mapped to actions as memorable cues: **None (sit), Ad hoc (crawl), Reactive (walk), Integrated (run), Proactive (fly),** and **Self-* (energise).**

The OAV Maturity Model (OAV MM) is offered by the Network eAcademy service in the form of a survey [OAV-MM-SURVEY] comprising 31 questions covering all technological and organisational aspects that should be considered in any transition to OAV. Survey respondents are issued a report providing a detailed analysis of their answers for each sub-dimension and a total maturity score for their organisation based on the defined stages, as well as an overall assessment of how their organisation compares to the average for the community in the various dimensions. The results for individual organisations are confidential and only aggregated and average results are published.

The OAV maturity assessment will help identify the areas which require more effort in order to achieve an efficient and scalable OAV implementation that is aligned with the overall strategy, supported by development and operations teams. Based on their maturity model report, an organisation will be able to decide the desired stage they would like to achieve in each dimension and sub-dimension: some possible actions may be seen as quick wins, others may be more complicated or time-consuming but may be worth the effort, while other areas may be marked as future tasks due to their lack of relevance to the organisation or amount of effort they require.

The goal of this white paper is to provide a better understanding of the maturity model's dimensions and stages and facilitate the evaluation and advancement of OAV. First, a definition of the stages is provided, followed by the definition of each dimension and sub-dimension, as well as the stages defined for each of the sub-dimensions. The definitions of the terms used in the sub-dimensions can also be found in the Terminology Document in the Network eAcademy [NA_eAcademy].

2 OAV Maturity Model Stages

The OAV Maturity Model defines six stages against which the levels of OAV maturity of organisations are mapped: None (sit), Ad hoc (crawl), Reactive (walk), Integrated (run), Proactive (fly), and Self-* (energise). These are illustrated in Figure 2.1 and described in the sections that follow.
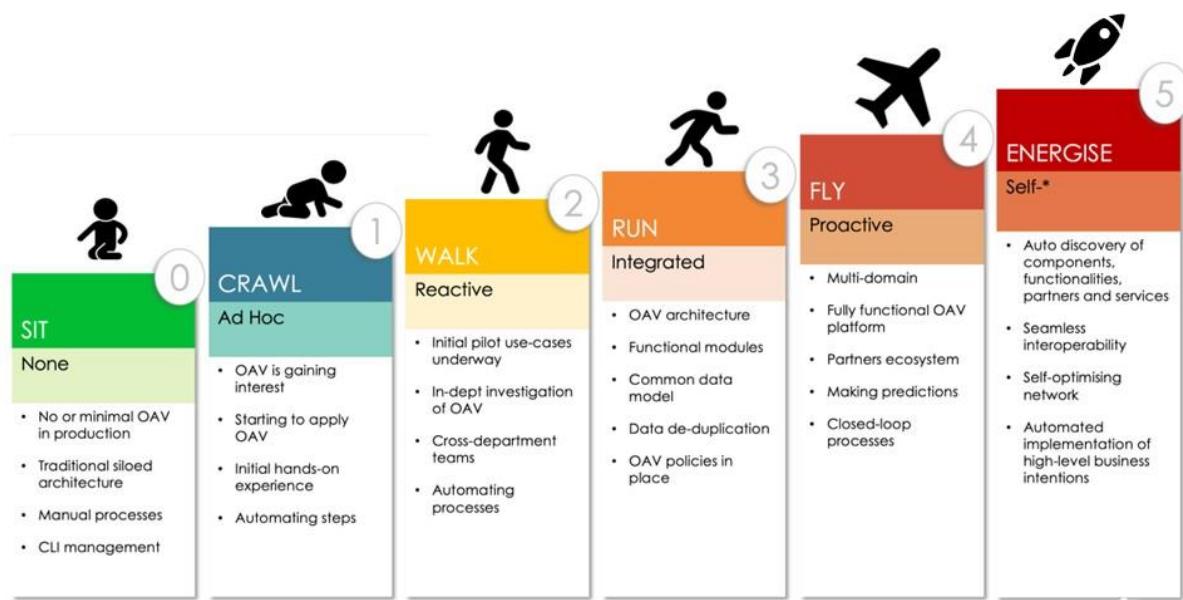
Figure 2.1: OAV MM stages

2.1 None (sit)

Organisations in this stage have either not implemented OAV in their production networks, or have only implemented minimal virtualisation. In the 'None' stage, the organisation's architecture is traditional with siloed tools, manual processes and CLI-based management. Vendor-compatible bundled solutions are used for advanced management. There may be some sporadic interest in using some of the OAV technologies, but these instances are isolated and are only used for personal or testing purposes. Employees and other relevant stakeholders may be starting to express interest in employing OAV technologies and related training activities.

2.2 Ad Hoc (crawl)

OAV has gained traction and there is interest among engineers and development teams. In the ad hoc stage, some individuals or small teams are starting to apply OAV in their production procedures to try and make their daily activities easier and less error-prone and the OAV capabilities of tools and suites are starting to be analysed. Some scripts are developed to automate steps in production processes. Policies and procedures are starting to change to incorporate aspects of OAV. Selected department members are investigating technologies such as

data analytics and AI and are gaining initial hands-on experience. Initial experimental virtual components are put into production.

2.3 Use Case/Project-Based – Reactive (walk)

OAV is now part of the strategic decisions of upper management and initial pilot use cases (at a service or process level) are being implemented in production. Several cross-departmental teams are being formed around the chosen projects and in-depth investigation and integration of management components is underway. The goal is automation of chosen processes by using (and if required, developing) compatible APIs and related data models. A virtual infrastructure is being set up in the production environment and virtual services are available for use. This leads to a gradual change in the organisational architecture – moving from a traditional closed/siloed approach to one using OAV functional components. The overall attitude of the organisation towards OAV is starting to change and trust in OAV technologies is rising. AI-based approaches and related advanced techniques are being sporadically used.

2.4 Integrated (run)

The organisation has now transitioned to an OAV architecture: all components in place can be managed and queried via exposed APIs that share a common data model – enabling full automation and orchestration of all processes in the production environment. A platform-based approach is used to manage the organisation's domain with well-defined functional components developed using decomposition and data deduplication techniques (e.g. there is a functional consistent single source of truth). All organisation policies and procedures are adapted accordingly. Hybrid (combined physical and virtual) services are also available in the service portfolio. The AI-based analytics enables fast response to alarms. All decision-making is based on high-quality data (accurate, complete, reliable, and relevant information that meets the specific needs and standards for its intended purpose). All stakeholders are invested in OAV and fully understand its values and benefits.

2.5 Proactive (fly)

The organisation is upgrading to an advanced multi-domain OAV platform for all services – aiming to achieve proactive behaviour in all aspects of its activities and to be ready to join an ecosystem of partners. All network services and devices (virtual and physical) are now fully compatible with each other and can be combined in flexible ways. Operations activities are all AI-supported, and the implemented predictions and closed-loop processes enable the organisation to always be one step ahead. Agility and customer experience are the main drivers for change.

2.6 Self-* (energise)

The organisation is exhibiting self-anything behaviour (systems and devices can autonomously manage and optimise their operations without human intervention, with self-monitoring, self-diagnosis, self-configuration, and self-healing capabilities allowing these systems to adapt, troubleshoot, and optimise themselves based on real-time data and changing conditions). New components, functionalities, partners and services are discovered automatically and interoperability is achieved in a seamless manner. The network is fully self-optimising and all management interactions take place on the basis of high-level business intentions. Self-service is brought to a new level – allowing users to define their own services and autonomously manage their lifecycle using self-healing features where necessary. Open collaboration based on high-level policies is established among ecosystems enabling self-composition of services across domains.

3 Dimensions and Sub-Dimensions of the OAV Maturity Model

The OAV Maturity Model additionally comprises four dimensions: Architecture & Technology, Processes & Services, Vision & Strategy, and People & Organisation, as shown in Figure 3.1. Each dimension in turn consists of different sub-dimensions. The stages set out and described in the previous section – None (sit), Ad hoc (crawl), Reactive (walk), Integrated (run), Proactive (fly), and Self-* (energise) – are defined for each sub-dimension.
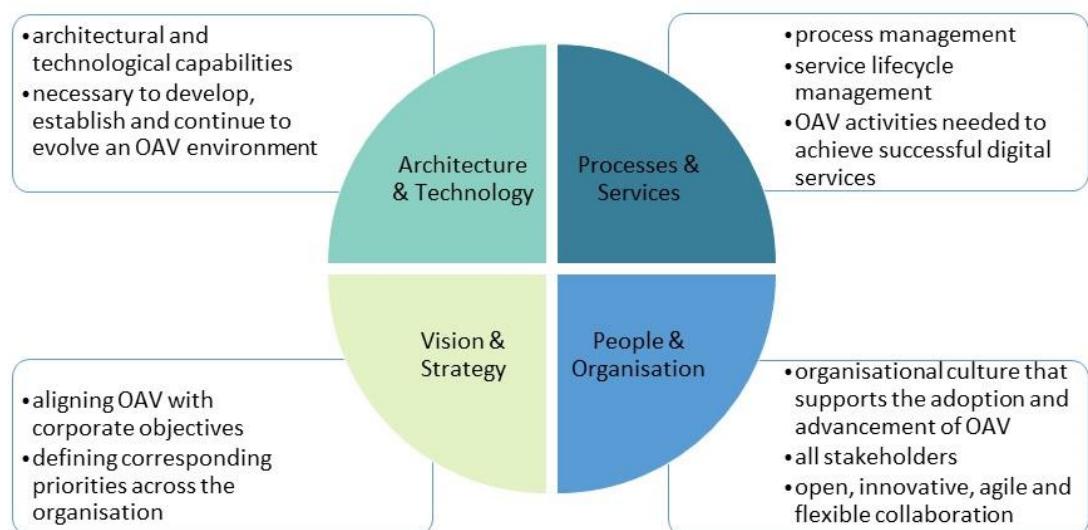
Figure 3.1: OAV MM dimensions

The concept behind the OAV MM is for it to be used as a self-assessment tool to help organisations identify strengths, weaknesses, opportunities and threats, by assigning a maturity stage to each dimension and sub-dimension, from which the overall maturity level for the organisation as a whole is extrapolated. Where an organisation is found to be at one of the lower stages of maturity for a specific sub-dimension, the MM can help to clearly identify areas of improvement and specific actions that can be taken to enable them to achieve a higher stage at their next assessment. Assessments can be taken periodically or ad hoc to check an organisation's evolution at a specific point in time.

Detailed definitions along with a visual guide of the six possible stages for each of the sub-dimensions are provided below.

OAV Maturity Model – Sub-dimensions

Architecture & Technology	Processes & Services	Vision & Strategy	People & Organisation
Components integration	General processes / automation	Policies	Teams development
APIS	Service lifecycle management	Data/Information governance	Stakeholders
Compatibility	Monitoring and reporting	Strategic approach	Building skills/expertise
Virtualisation	Troubleshooting	Service management	Culture
Security	Security management	Agile capability	User / customer experience
Data modelling/object abstractions	Service design	Standardisation	
Analytics		Investments	
AI			
Data			

Figure 3.2: OAV MM sub-dimensions

3.1 Architecture and Technology

This dimension describes the architectural and technological capabilities that are necessary to develop, establish and continue to evolve an OAV environment capable of implementing the organisation's objectives. It focuses on OAV platform flexibility and interoperability, modularity and APIs, virtualisation technologies, modelling capabilities, AI-powered data analytics, and efficient and adaptable resource leverage.

Given the technology-oriented nature of the OAV MM, Architecture and Technology is the dimension that has the greatest number of sub-dimensions. These sub-dimensions include components, APIs, compatibility, virtualisation, security, modelling abstractions, analytics, AI, and data.

3.1.1 Components

A component is a functionally independent part of any system. It performs some function and may require some input or produce some output. The six stages of maturity for this sub-dimension are defined below.

None

The organisation uses closed, separated components for different purposes, with a traditional siloed approach where different services and types of devices are managed independently. Specialised components are used for the management of groups of devices (usually vendor-provided tools) and vendor-issued suites may be used for advanced network management. There are some functional and data overlaps between components.

Ad Hoc

In the ad-hoc stage, sporadic cases of component integration are implemented on a small scale and data extracted from one component is used in another component. Examples include pushing relevant information to a monitoring component to autostart monitoring after service provisioning or attempting to auto-generate a service-specific report using data available in several independent components.

Use Case/Project-Based – Reactive

In this stage, all components that are used in a defined use case or project are being integrated so that they can easily exchange information. Any functional duplication is being avoided and decisions are being made on which component is going to provide which functionality. Data deduplication is being investigated for the identified components. A vendor-neutral approach is emerging. The organisation is moving away from siloed architecture.

Integrated

In the integrated stage, all components within the organisation are integrated, and a platform is established. The definition of organisation-wide functional components where each component provides well-defined functionalities (e.g. single source of truth) is achieved in a vendor-free manner. To implement complex behaviour, multiple functionalities can be used in a process. All service and device management can be done using these functional components. In this way, the organisation has abandoned the siloed approach and is now establishing an OAV platform that responds to user requests and network managers' actions.

Proactive

In the proactive stage, the components are available as services listed in a service catalogue and a platform is fully functional. All functional components can now be used as flexible puzzle pieces, where each functionality is advertised in a component catalogue. Dynamic integration is possible by searching components and combining them using an intelligent orchestrator. Each component not only exposes a management API but also provides
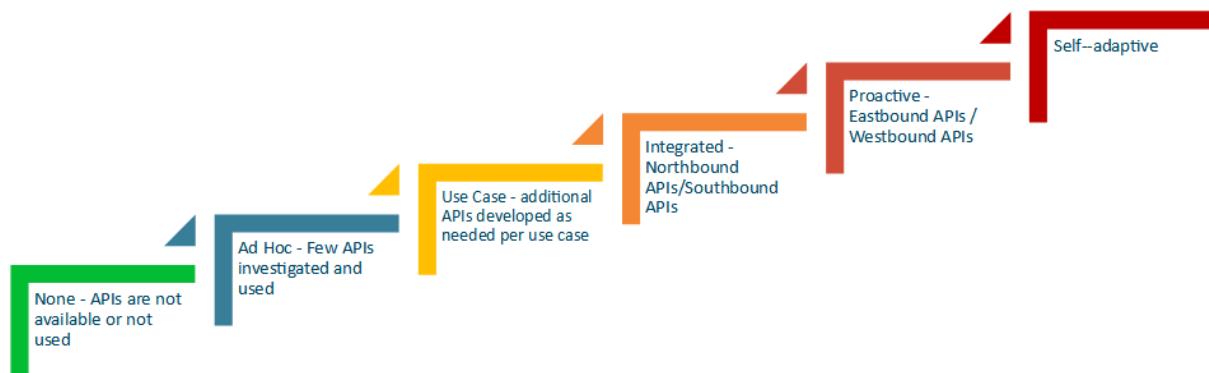
notification capabilities – thus supporting the definition of process choreography with message exchanges leading to higher levels of collaboration.

Self-*

For the 'components' sub-dimension, self-* indicates that all platform components are easily discoverable by internal and external parties (intelligent self-discovery). They intelligently respond to the addition or removal of other components and are adaptable to a changing environment, e.g. auto-discovery of relevant information stored in federated inventories on the fly.

3.1.2 APIs

An API is a set of commands, functions, protocols, and objects that programmers can use to create software or interact with an external system. Any data can be shared with an application program interface. The six OAV MM stages for the API sub-dimension are described below.

None

In this stage, the organisation does not use APIs to interact with components/tools. Only available GUIs and readily available exporting/importing facilities are used. Many of the tools/components might not expose APIs at all.

Ad Hoc

Ad-hoc interest in component APIs is growing as a few APIs are investigated and used. Some existing APIs are now being used for small automated tasks. Available APIs may follow different paradigms (REST, SOAP, etc.).

Use Case/Project-Based – Reactive

An API analysis is performed for the components chosen to implement the selected process. Additional APIs or API extensions/wrappers may be developed for certain components to facilitate automation and data exchange. The organisation is becoming aware that a standardised approach to APIs is needed. A common API definition guide is being developed.

Integrated

Following the API guidebook, all components are now exposing standardised (preferably open) APIs that are based on a common data model. Using the available APIs, the organisation is able to define workflows in both directions: from user to network (Southbound) and from network to user (Northbound).

Proactive
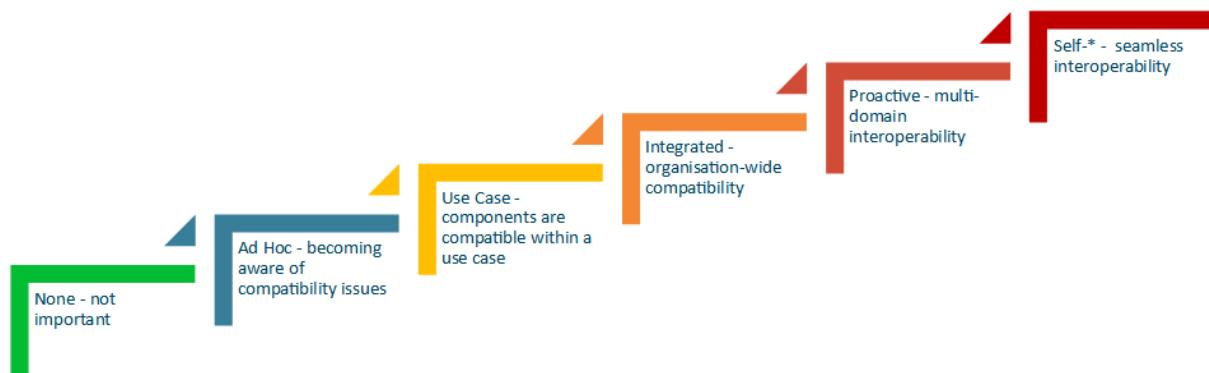
The organisation exposes external APIs that can be used by customers and partners. Standardised Open East-West API specifications are used for these purposes. An API Gateway is established with full access control and accountability – redirecting calls to the internal APIs. A Notification Broker (following the Pub/Sub paradigm) is implemented for all services.

Self-*

The organisation uses adaptive APIs that dynamically adapt its control and display features to react in real-time to different user, system or environment states. Machine-to-Machine communication is fully supported.

3.1.3   Compatibility

In this survey, compatibility is defined as the ability of software and hardware from different sources to work together without having to be altered to do so. The stages for the Compatibility sub-dimension are as follows:

None

Compatibility between different tools/management components is not required – nor is it investigated. Compatibility of network devices is important only in terms of providing service.

Ad Hoc

The organisation is becoming aware of compatibility issues, as ad-hoc attempts at integration start to be made, compatibility issues begin to surface, and workarounds are proposed. This awareness influences future considerations regarding new hardware/software purchases.

Use Case/Project-Based – Reactive

While attempting to automate particular processes, the compatibility between the identified/involved components is addressed. Customised extensions or additional software implementations are used to enable interoperability between the components in question. The use of common models and data duplication issues are starting to be addressed.

Integrated

All components and tools that are used to implement the processes in the organisation are now fully compatible and interoperable. Standards and models are chosen to ensure compatibility with development efforts in progress or future procurements.

Proactive
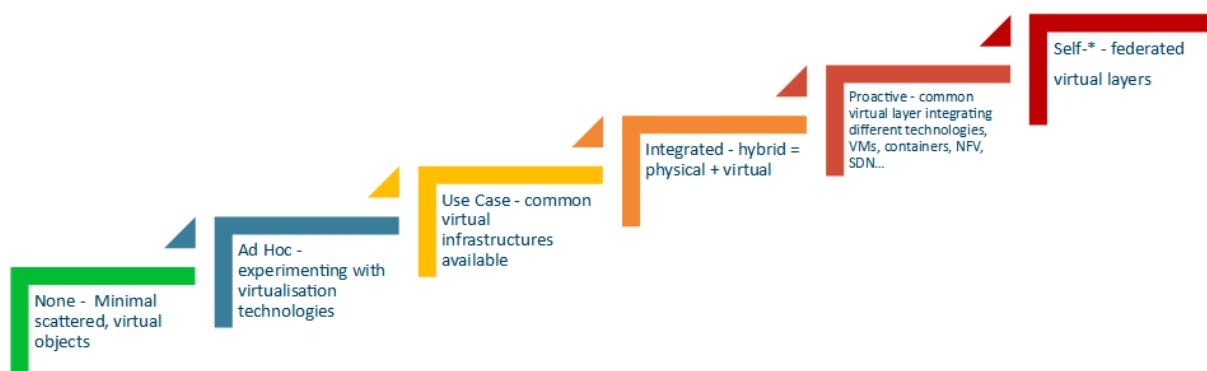
The organisation is now interoperable with other partners and can easily exchange information with their systems. Remote (controlled) auto-triggering of its processes is also provided to the partners based on common agreements, standards and regulations.

Self-*

The organisation can establish interoperability agreements with a selected partner on the fly – intelligently adapting the communication channel between the organisations. Smart contracts can be used to define agreements.

3.1.4   Virtualisation

Virtualisation is the abstraction of network or service objects to make them appear disassociated from the underlying hardware implementation specifics. The maturity stages of virtualisation are:

None

The use of virtualisation technology is minimal – there is no common virtualisation platform in use. There may be VPNs in place, a few proprietary, vertically integrated boxes available in the network or individually managed VMs hosting a few services.

Ad Hoc

Awareness of the need to choose common virtualisation platforms is rising. Examples are used to understand virtualisation abstractions and implications. There are a number of isolated virtual deployments of standalone VMs, containers and/or VNFs.

Use Case/Project-Based – Reactive

A common virtualisation platform is chosen and implemented. There is now support for multi-vendor VNFs and horizontal scalability of virtual objects. Some services are transferred to virtual hosting. There is a clear distinction between virtual and physical objects.

Integrated

Physical and virtual components are now interoperable and hybrid services can be implemented. Hybrid services in virtualisation combine on-premises infrastructure with public cloud resources, offering a flexible and scalable solution that balances control, cost, and innovation. Network service chaining is in use for production network services. Virtual network services can be orchestrated using an NFV orchestrator. Implementations are being scaled vertically (the main difference between horizontal scaling and vertical scaling is that horizontal scaling involves adding more machines or nodes to a system, while vertical scaling involves adding more power (CPU, RAM, storage, etc.) to an existing machine).

Proactive
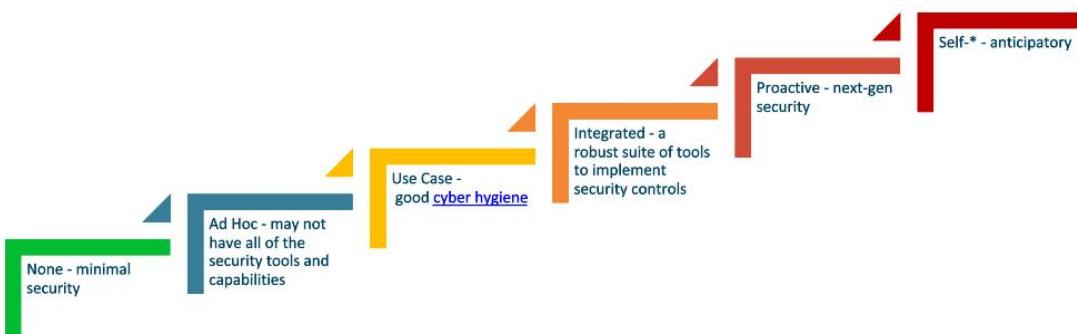
A common virtual layer is available that provides complete end-to-end network visibility, overarching different technologies and implementations (VMs, containers, NFV, SDN…). The organisation has a fully virtualised environment with auto-scaling support: desktop, application, network, storage, and data visualisation.

Self-*

The common virtualisation layer transcends the organisation domain/control and federates with other virtual infrastructures that belong to partner organisations in a fully transparent manner using next-gen virtualisation technologies.

3.1.5   Security

In this context, security signifies a set of measures, systems, solutions, tools and procedures that are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organisation [Cisco Web]. With reference to Security, the following six stages are defined.

None

In the None stage, the organisation manually configures the prevention-oriented tools (e.g., firewalls, antivirus software, etc.) it has in place. There is no defined security architecture and changes are implemented on individual systems. Logs are stored locally and managed by separate security tools.

Ad Hoc

Basic network security perimeters are established where trust is mostly assumed within the owned network. Log data and security events stats are exported to a centralised server. Endpoint security is starting to be implemented in a consistent manner. There is no common framework to cover all OAV-related security aspects.

Use Case/Project-Based – Reactive

In this stage, a robust suite of tools to implement security controls is in place. A centralised architecture has been developed where all log data and security logs are made available in one location. Automated configuration of prevention-oriented security equipment is the norm. Security policies (password expiration, password hardening, etc.) are enforced. Mandated network forensics are gathered.

Integrated

A centralised architecture has been realised with endpoint/edge security devices, analysis of the monitoring data for security threat analytics, endpoint forensics and prioritisation of alarms. Security equipment has been commissioned with automatic configuration based on threat and risk assessment in a reactive manner. The target in this stage is to secure all physical and virtual assets in areas of higher risk. The organisation has a resilient and highly effective compliance posture. All Security Operations Centre (SOC) functionalities are in place.

Proactive

With the growing number of components that need to be secured, a shift towards decentralised architecture is made, with distributed security devices. A Security Information and Event Management (SIEM) system is used to holistically analyse the distributed log events data based on Indicators of Attack (IOA) and Indicators of Compromise (IOC) for known threats. Targeted advanced analytics for anomaly detection and endpoint forensics are used. Security equipment setup is based on threat and risk evaluation with automatic configuration in a proactive manner.
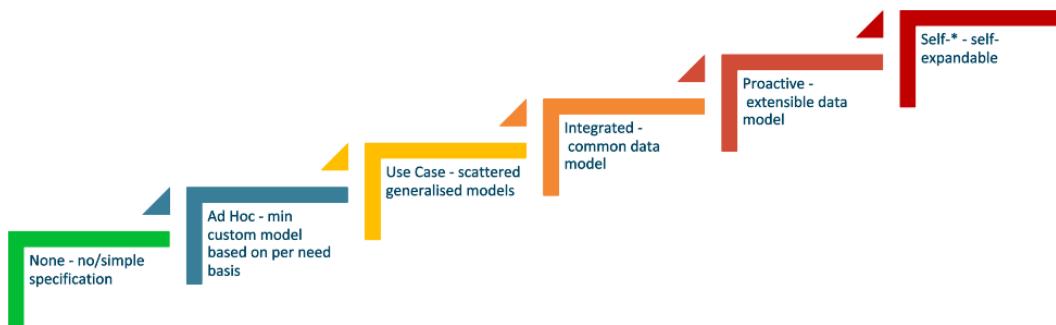
Self-*

The Self-* stage for Security is anticipatory, using a decentralised architecture with distributed security devices. Analysis of the monitoring data is advanced, is based on IOA and IOC for known threats on the security devices, and uses AI/ML and federated learning. Security devices execute alerting with holistic network forensics and Tactics, Techniques, and Procedures (TTPs)-based scenario machine analytics for known threat detection. Advanced machine analytics is used for holistic anomaly detection (e.g., via multi-vector AI/ML-based behavioural analytics). Cross-organisational case management and automation, as well as extensive proactive capabilities for threat prediction and threat hunting, are in place. The organisation has an extremely resilient and highly efficient compliance posture. The security equipment setup is self-configurable.

3.1.6 Modelling Abstractions

A data model (or datamodel) is an abstract model that organises data elements and standardises how these relate to one another. Modelling abstractions refers to the process of simplifying complex real-world data structures into more manageable, often simpler, conceptual representations. This process involves stripping away unnecessary detail and focusing on key attributes and relationships to create a blueprint or framework for systems to understand and manage data.

The role of modelling abstractions is critical in understanding and representing data in a structured manner. Without such abstractions, the intricacies of real-world data can become overwhelming, leading to inefficiencies, errors, and confusion. By creating a standardised and simplified representation, data models ensure consistency, predictability, and clarity. Data models are essential because they provide a foundation upon which database designs, data architectures, and software applications are built. They serve as a roadmap for developers, data architects, and database administrators, ensuring that everyone works from a consistent blueprint. The maturity stages in this area are described below.

None

In this stage, there is no attempt to define the specifications or abstract models of resources/objects of interest (services, devices, metrics, etc.). The readily available models provided in the tools/components are used with very little or no customisation.

Ad Hoc

The initial steps in automation and integration lead to the need to define initial data models and specifications that will be used to understand the data flow in/out of components. The models employed are rudimentary with low granularity and very difficult to extend. There are a few attempts to distinguish between logical and physical object modelling.

Use Case/Project-Based – Reactive

The requirement for a common approach to object modelling is recognised. Modular models are being defined. Hierarchical composition and abstractions are considered.

Integrated

The organisation has a functional data model that can be used to describe physical and logical objects and their relationships. A standardised approach to object specification is used.

Proactive

The data model is now easily extensible with custom object parameters. A highly granular approach is implemented, so that objects can be constructed using a number of hierarchically arranged modules. Multi-layered abstractions can be described, enabling the definition of different views (complete, partial, limited with fine control) of the organisation's resources.

Self-*
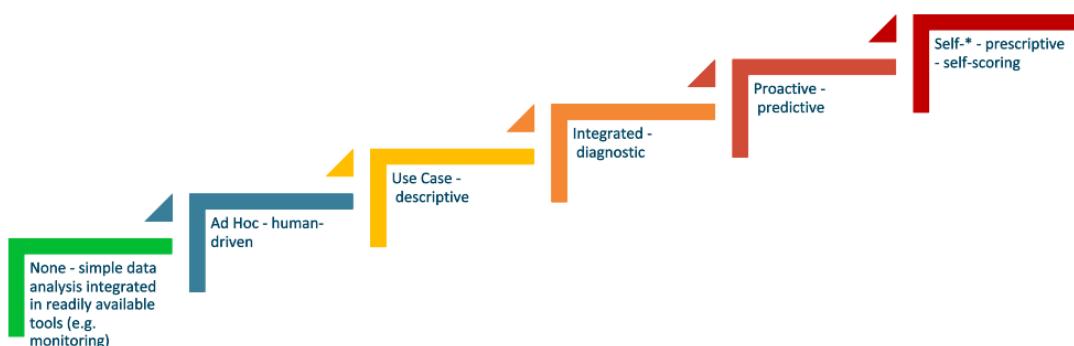
The object models can be extended on-the-fly. New abstraction layers can be auto-generated based on a mix of intentions and controls. Model definition can be learned and optimised by the system.

3.1.7   Analytics

Analytics is a field of computer science that uses mathematics, statistics, and machine learning to find meaningful patterns in data. Through the use of analytics, organisations describe, diagnose, predict and prescript, and are able to make well-informed decisions on the allocation of resources, optimisation of processes, and configuration of systems. [SAP Web]

In the context of OAV , analytics can be employed to assess workflows and identify optimal sequences, hence mitigating bottlenecks and minimising system latency, identifying   recurring processes or inefficiencies, or allocating virtual resources in accordance with real-time demand, hence optimising performance and minimising expenses.

The stages of maturity relating to analytics are defined in the following sections.

None

There are no specific analytics tools in use. Only the readily available data visualised in different tools is used. Basic statistical information is provided but not analysed automatically.

Ad Hoc

Basic analytics tools are used on historical data gathered by exporting/importing different databases/sources. There is no integration between the analytics tools and the data sources. Analytics is usually performed for the purposes of reporting or capacity management at given time intervals. No real-time analytics is provided.

Use Case/Project-Based – Reactive

Real-time data analytics together with relevant statistics are provided using a centralised analytics tool. Statistical data analysis is performed to understand what happened in the past and current performances, using visualisations, reports and dashboards.

Integrated

Automated root-cause analysis is employed. Deeper analysis is performed on the descriptive data to be able to understand why events, incidents or problems are   happening. The process includes data discovery, data mining, drilling down and drilling through.

Proactive

Historical data is fed into learning models that analyse trends and patterns. When combining the model with real-time data, predictions on the future behaviour of the infrastructure, future incidents and problems, the occurrence of security threats, etc.
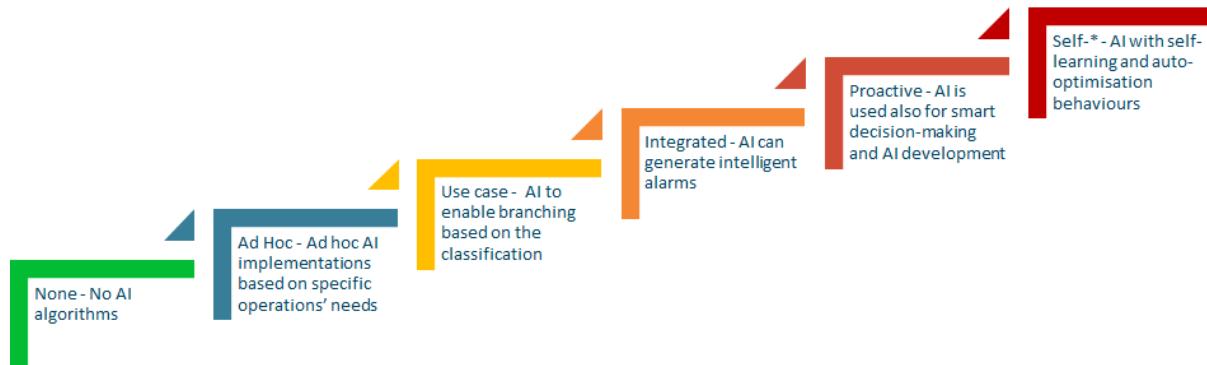
Self-*

Engines make smart decisions by analysing what actions can be taken to affect the forecasted outcomes. Predictive data is used to automatically generate options on different courses of action (prescriptions) together with an impact analysis of applying each option.

3.1.8   AI

Artificial Intelligence (AI) is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. It is a system's ability to correctly interpret external data, to learn from such data, and to use that learning to achieve specific goals and tasks through flexible adaptation.

In the context of OAV (Orchestration, Automation, Virtualisation) systems, the integration of AI is anticipated to mostly occur in domains that have the potential to improve efficiency and responsiveness. Artificial intelligence can provide real-time support in making decisions for orchestration, thereby ensuring the most efficient workflow sequences in response to dynamic conditions. It also   possesses the capability to forecast and adapt processes, thereby mitigating the likelihood of errors and progressively enhancing the execution of activities. In the realm of virtualisation, artificial intelligence   can enhance resource allocation by accurately forecasting the most optimal configuration for certain workloads. Furthermore, the utilisation of AI-powered analytics enables the continuous monitoring and comprehensive analysis of system health, performance, and security, hence the taking of preemptive measures to mitigate potential issues before they reach a critical state. The stages of AI maturity for organisations are defined as follows:

None

AI solutions are not used at all, and no AI algorithms are in place for detection, classification or predictions.

Ad Hoc

Initial investigations into the use of AI are starting. Ad-hoc AI implementations are available based on specific operations' needs, usually for reporting purposes.

Use Case/Project-Based – Reactive

AI is being piloted in chosen projects. Some processes are coupled with AI solutions to enable branching based on classification. All AI deployments are carefully supervised to ensure consistent behaviour.

Integrated

Some AI modules are integrated into several cross-department processes. AI is used to generate intelligent alarms based on the recognition of hidden patterns using unsupervised approaches to learning.

Proactive
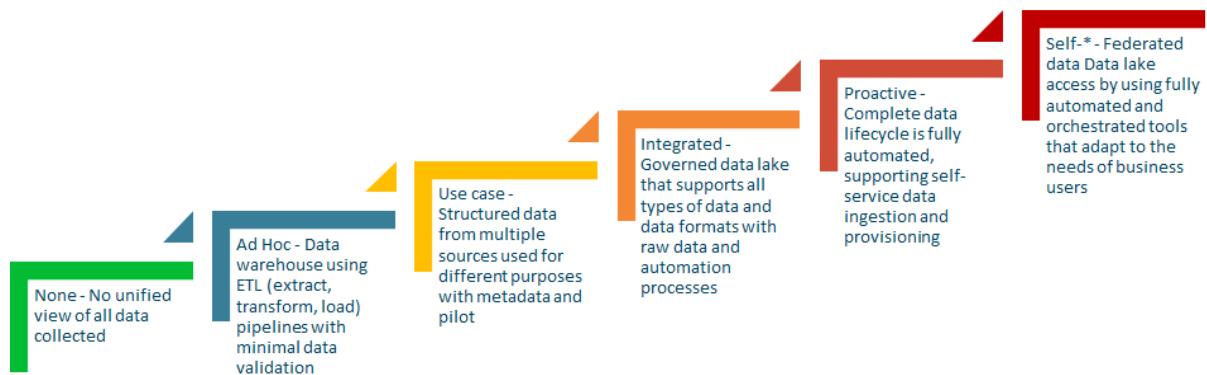
In this stage, AI is used in most of the organisation's processes not only for classification purposes but also for smart decision-making. A central AI platform is used to manage the lifecycle of all AI deployments. A standardised approach to AI development is adopted.

Self-*

AI is used as the innovation driver in the organisation leading to fully autonomous systems that work according to pre-defined intents. AI deployments are characterised by self-learning and auto-optimisation behaviours. For instance, AI can monitor network traffic and adjust QoS settings on-the-fly to prioritise critical applications or services, or can detect anomalies in network traffic, pointing at potential security threats or issues and automatically blocking malicious traffic or isolating compromised devices.

3.1.9   Data

Data are facts and statistics collected for reference and analysis [Data Definition]. Organisations   may for example collect data relating to user behaviour, content consumption patterns, or system performance. By analysing data, companies can derive insights that enable them to optimise content delivery, enhance user experience, address system inefficiencies, and predict future trends. The stages of data maturity of organisations are defined as follows:

None

Structured data is collected and stored in a number of databases based on its purpose and the tools used for its collection. Each datastore follows its own rules regarding data structure, format, naming conventions etc. There is no unified view of all data collected, and combining data from different sources and/or formats is difficult.

Ad Hoc

A centralised data infrastructure in the form of a data warehouse or similar is used. Data can be processed using ETL (extract, transform, load) pipelines where at least minimal data validation is performed when integrating data from multiple systems. Metadata repositories are starting to be used, and unstructured data is not collected.

Use Case/Project-Based – Reactive

An enterprise data warehouse is used as a data hub supporting business intelligence. Structured data from multiple sources across all organisation processes is stored and used for different purposes such as reporting, analysis, dashboards, etc. Metadata provides access to end-users for searching and understanding data. Pilot data lakes may be in place to take advantage of semi-structured and unstructured data for project-based analytics efforts.

Integrated

A governed data lake is used to set up an advanced data environment that supports all types of data and data formats. Raw data is stored for different types of analytics where schema on the fly is employed. Automation processes related to the whole data lifecycle are being put in place.

Proactive

A unified, optimised, intelligent data lake is being used with a virtualisation layer set on top of all data stores in the organisation, creating a single cohesive environment. The complete data lifecycle is fully automated, supporting self-service data ingestion and provisioning. Data stewards ensure the quality of the data used by the organisation.

Self-*

Federated data – either in data lakes or in a data mesh – are in use. Data from various sources in the

ecosystem (e.g. other partner organisations) can be accessed and used in combination with the local responsive data lake. Access and insight into the available data without the need for any special technical support is made possible by using fully automated and orchestrated tools that adapt to the needs of business users.

3.2 Processes and Services
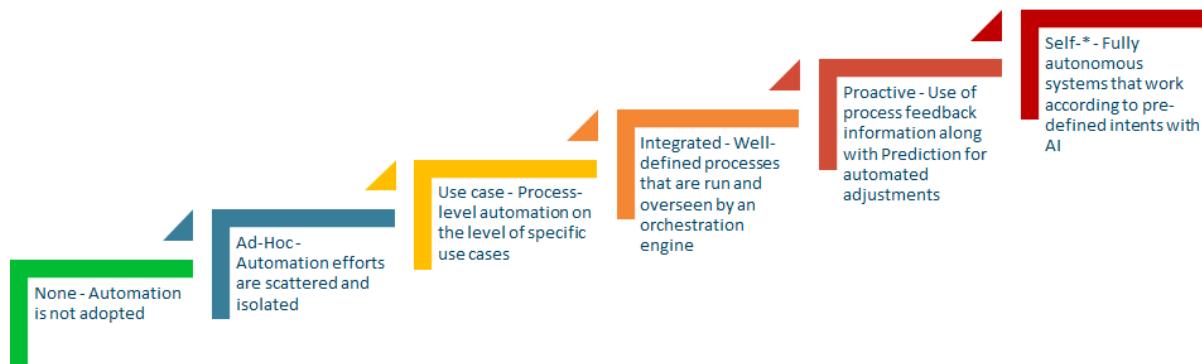
The second maturity model dimension relates to the process management and service lifecycle management of OAV activities that are needed to achieve successful digital services. The OAV approach extends beyond network operations and encompasses organisation-wide procedures and processes. Combined with standardised elements and optimisations in all processes and services, OAV aims to create an efficient and continuously evolving organisation environment.

The sub-dimensions for processes and services aim to capture the maturity of process automation and service specification in general, with additional sub-dimensions focusing on different aspects of the service lifecycle. These include   automation of processes, service design, service lifecycle management, monitoring and reporting, troubleshooting and security management.

3.2.1   Automation of Processes

Automation refers to processing tasks in a repeatable manner to yield the same result every time, without human intervention.

Process automation refers to the usage of technology to automate complex processes. It typically has three functions: automating processes, centralising information, and reducing the requirement for input from people. It is designed to remove bottlenecks and reduce errors and data loss, all while increasing transparency, communication across departments, and processing speed. The process automation MM stages are:

None

In the None stage, automation has not been adopted by the organisation or by individuals. Configuration is done manually using element management interfaces (CLIs or GUIs). Integrity is completely dependent on engineers.

Ad Hoc

Automation efforts are scattered and isolated. Single repetitive time-consuming tasks such as updates are automated by devising individual automation scripts that are then run when needed. These approaches are not coordinated in any way.

Use Case/Project-Based – Reactive

Task-specific automation is evolving into process-level automation at the level of specific use cases (projects) being implemented.

Integrated

Direct element configuration is abandoned; well-defined processes that are run and overseen by an orchestration engine are now in place. Integrity is guaranteed using input validation and a "single source of truth" approach. Implemented processes are able to guarantee stable configuration and correct information regardless of whether the process has been completed successfully or has failed (graceful exit).

Proactive
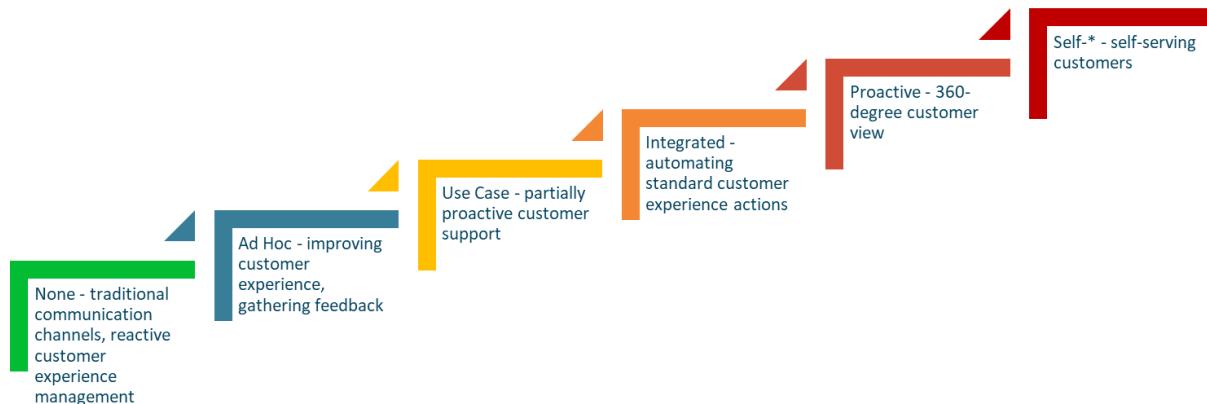
Continuous improvement is implemented using process feedback information. The initial steps towards the implementation of closed control loops are being implemented. Prediction information is used to make automated adjustments.

Self-*

AI is used as the innovation driver in the organisation leading to fully autonomous systems that work according to pre-defined intents. AI deployments are characterised by self-learning and auto-optimisation behaviours.

3.2.2   Service Design

Service design provides guidelines and best practices for designing new IT processes and services and preparing them for a live environment. The maturity stages of service design are summarised below.

None

Formal/informal service configuration procedures are available, outlining the actions that need to be taken to manage a specific service. Service descriptions in the service portfolio are available only in text format. Services are not described in a standardised manner.

Ad Hoc

Technical service specifications are available. Data modelling languages are being investigated in sporadic attempts to create a formal service specification definition. Service design practices such as "customer journeys" are being explored.

Use Case

Chosen pilot services are being defined using service design practices. Data models are being built around these services and their service parameters are being defined (e.g. using YANG or XML).

Integrated

Service design is embedded in the day-to-day activities of the organisation. Parameterised service specifications exist for all services in the service catalogue and they are available in a machine-readable format ready to be consumed by different functional blocks. Specification activities follow a common approach. Resource Facing Services (RFS) and Customer Facing Services (CFS) are recognised as necessary.

Proactive
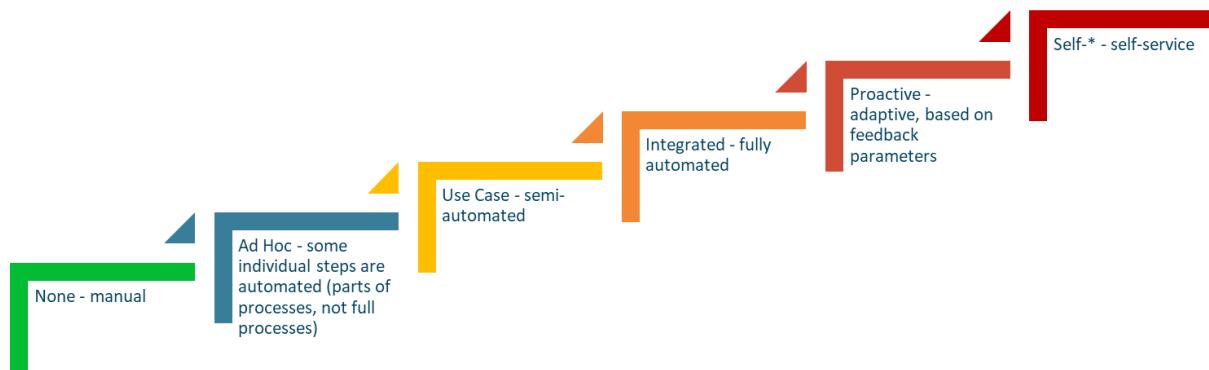
Service specifications are defined as a combination of highly granular puzzle pieces that represent different parts of a resource-facing or customer-facing service. New services can be designed using readily available puzzle pieces.

Self-*

Users become active participants in service design and can build their own custom services using available service puzzle pieces in a flexible manner. The service design process is fully automated and streamlined to optimise the customer experience.

3.2.3   Service Lifecycle Management

Service lifecycle management is a process of managing and optimising the complete life cycle of a service, from its conception stage to its retirement [The Tech Edvocate]. The stages of maturity of organisations for the service lifecycle management sub-dimension are described below.

None

All necessary service lifecycle management actions (device configuration, inventory record keeping, ticket updates, billing, etc.) are done manually.

Ad Hoc

Members of the operations team have started to automate specific tasks that are part of the service lifecycle management processes in order to save time or increase reliability. For instance, instead of manually handling daily data backups, a team member might craft a script to streamline the process.

Use Case

The service lifecycle management processes for certain services may be fully automated and the processes may be different for discrete services. There still may be manual steps in the process that require human confirmation – regarding configuration or other sensitive changes – because operational staff do not trust the automated process.

Integrated

All services are now managed in a fully automated fashion using well-established common processes. A self-service portal for end-users may be in place providing key information related to service instances.

Proactive

Service lifecycle management processes are able to adapt to the current network state. For example, if a problem is encountered during the implementation of the main process workflow the system tries alternative ways to complete the process successfully before giving up and reporting a failure.

Self-*
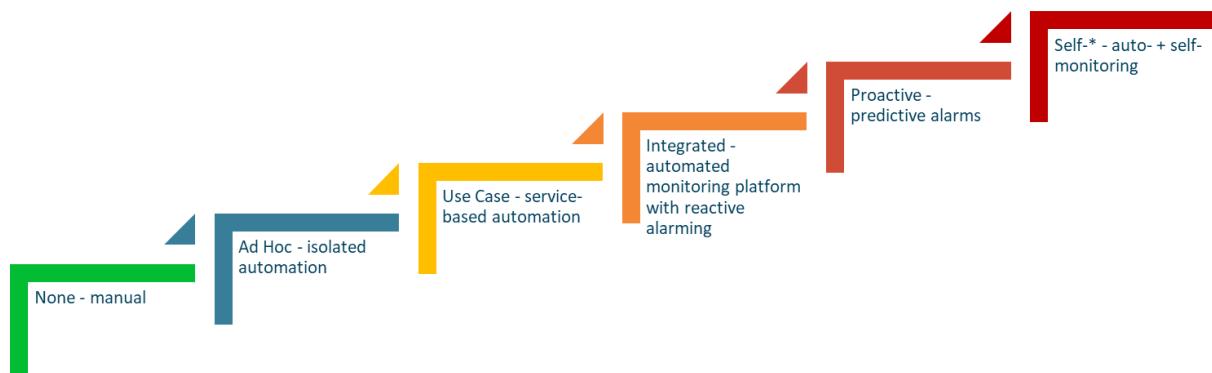
Fully-fledged self-service management is available where users only need to express their high-level intentions; everything else is inferred by the system. Orchestration processes are implemented using intelligent branching based on gathered information and analytic inputs.

3.2.4   Monitoring and Reporting

Monitoring is the observation and measurement of several parameters (from the link status or traffic on an interface or line to physical parameters such as temperature, humidity, etc). Reporting is the representation of data sources for reference and statistics [SIG-NOC Tools Survey].

Monitoring and reporting are key to business operations as they enable early problem detection and informed decision-making. Monitoring offers continuous observation of system parameters, ensuring timely interventions to maintain optimal performance, while reporting consolidates this data, providing stakeholders with clear insights into systems health and trends.

These practices transition from sporadic and manual to automated and predictive as organisations evolve, enabling them to respond proactively rather than reactively. This progression not only ensures operational efficiency but also fosters accountability, resource optimisation, and compliance with industry standards and regulations.

None

There may be a multitude of different monitoring tools, which work in silos. Tool configuration and alarm definitions are done manually.

Ad Hoc

Monitoring is housed within multiple, independent systems. There are dedicated monitoring tools that cover a number of technologies. There is some automation involved when it comes to preparing regular reports.

Use Case

Service end-to-end visibility is available for certain use cases. Monitoring tools are being consolidated. The start/end of monitoring of chosen services is done automatically. Reporting for these services is also automated.

Integrated

Every service/resource is automatically registered and classified on an overarching monitoring platform. The infrastructure – network, compute and storage – is seen as one unified view. Reporting is fully automated.

Proactive
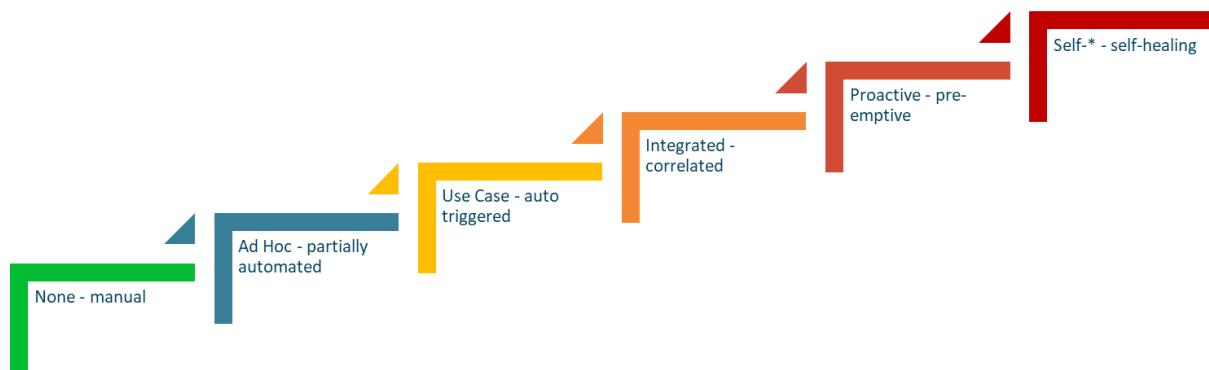
Proactive service-level monitoring is in place. In addition to real-time context-aware monitoring information, alarms are now predictive and provide information about potential future alarms based on AI modules. Instant detailed reporting is made available automatically.

Self-*

In the self-* stage, the monitoring system requires no human intervention. The monitoring platform constantly learns from multi-user and multi-domain datasets. Anomalies are detected long before they become problems. User-customised reporting is automatically generated.

3.2.5   Troubleshooting

Troubleshooting is a systematic approach to solving an incident or a problem [IBM Web]. The stages of maturity in this are shown below.

None

In this stage, troubleshooting is done manually and in a very limited context. For example, too many unnecessary changes can be made in a network, resulting in alarm storms which would then cause some critical alarms to

become hidden or be overlooked by the operational team. Correlation of information from separate systems is extremely difficult.

Ad Hoc

In this stage, there is partial automation. Teams still need to consult multiple tools and datasets to troubleshoot issues. Root-cause identification is very difficult since correlation is still performed manually. Automation is found mostly in ticket management procedures.

Use Case

Dashboards are used to provide a combined view of service information. Some alarms are recognised as related to the same service and are combined automatically.

Integrated

Troubleshooting is done using a single data pool. There is some small degree of machine learning implemented in the troubleshooting workflows – but no predictions yet. Root-cause analysis is automated.

Proactive
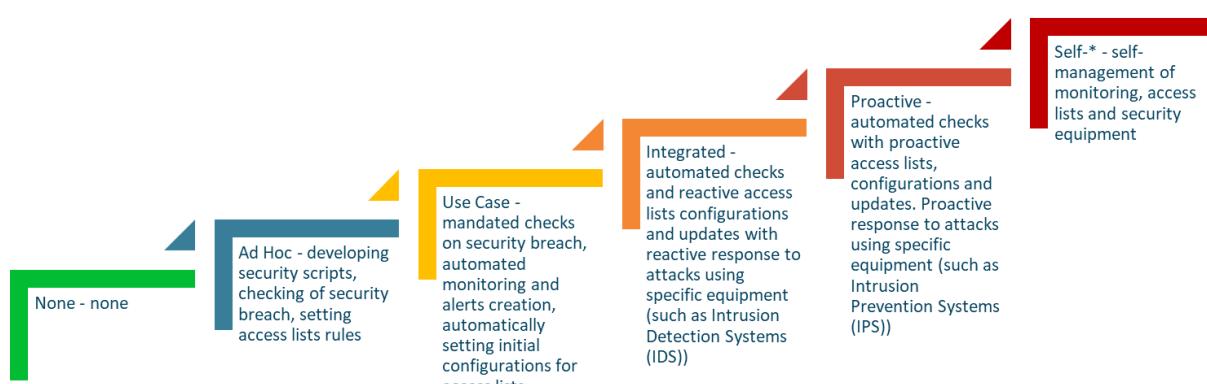
Machine learning is used to extract essential insights from large pools of operational data. Predictions are made regarding potential issues and mitigative steps are taken to avoid degradation. Root-cause analysis and remediation are automated.

Self-*

The system analyses data and repairs issues on its own. Failover is fully automated. Issues are resolved without any user input. Data and rules for self-healing algorithms are in use.

3.2.6   Security Management

Security management is a continuous process that describes the structured implementation of security within an organisation, and is assessed according to the following maturity stages:

None

Isolated security logging takes place in functional silos. There is no formal incident response process. The organisation is unaware of threats – whether internal, external or advanced persistent threats (APT).

Ad Hoc

Developing security scripts, checking for security breaches and setting access list rules are in place. There is no formal incident response process and there are no processes to manage security compliance violations. Some security activities are automated using simple scripts. The organisation is unaware of APTs and most threats.

Use Case

There is minimal compliance mandated for monitoring and response. A process to manage security compliance violations is in place. Automation is used to set up the initial security configurations. The organisation is still unaware of most threats and there is no formal incident response process.

Integrated

The organisation performs automated checks and reactive access list configurations and updates with reactive responses to attacks using specific equipment (such as Intrusion Detection Systems (IDS)). The threat intelligence lifecycle is reactive and manual. Basic monitoring and high-risk alarm processes are automated. A basic incident response process is established. There is good visibility of threats. Automation is now extended to reactive adapting of security configurations based on threat alerts.

Proactive

There are automated checks with proactive controls/access lists, configurations and updates in place. The response to attacks is proactive, using specific equipment (such as Intrusion Prevention Systems (IPS)). There are formal and mature monitoring and response processes with standard playbooks for most common threats. There is a targeted automation of investigation and a mitigation workflow. Effective processes are in place for the monitoring of alarms. The organisation does proactive threat hunting. Automation is leveraged to improve the efficiency and speed of threat investigation and incident response processes.

Self-*

In this stage, the organisation carries out self-management of monitoring, access lists and security equipment. There are established, documented and mature response processes with standard playbooks for advanced threats (e.g. APTs) in place. There is extensive automation of investigation and mitigation workflow and full automation – from qualification to mitigation – for common threats. Automated threat qualification, investigation, and response processes are in place wherever possible. All classes of threats are recognised and quickly responded to early in the Cyber Kill Chain.
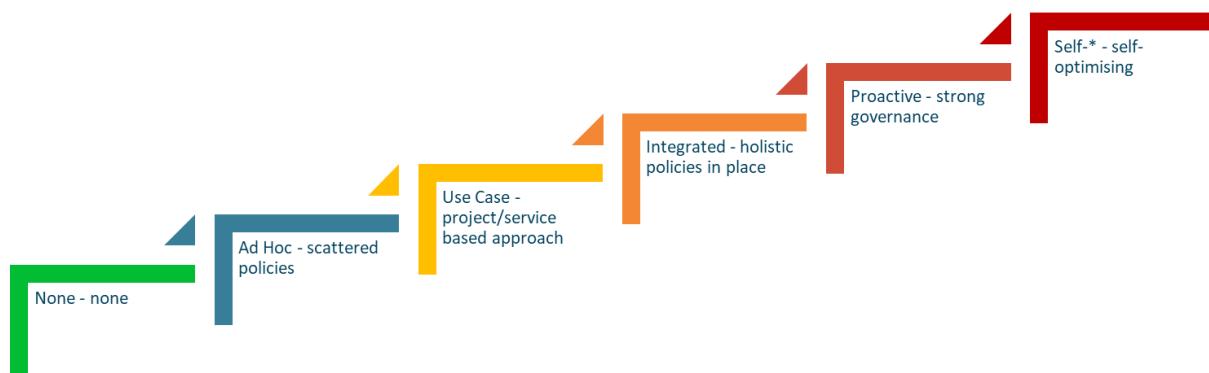
3.3 Vision and Strategy

The main focus of this dimension is the development and management of an OAV vision and strategy – aligning OAV with corporate objectives and defining corresponding priorities across the organisation. It includes information governance, policy definition and implementation, strategic decision-making, financial aspects and any other aspects of OAV as a business enabler, such as agility, standardisation or service management.

The subdimensions defined in the Vision & Strategy dimension are as follows:

3.3.1 OAV Policies

An OAV policy is a statement of intent regarding OAV and is implemented as a procedure or protocol. The following stages of maturity are considered for OAV policies:

None

There is no common ground in OAV-related work activities. No formal policies regarding OAV development and implementation are defined.

Ad Hoc

The need for common OAV development and implementation policies is starting to be recognised. Attempts to develop OAV-related policies are underway. A minor set of OAV policies is used operationally.

Use Case/Project-Based – Reactive

OAV development and implementation policies are developed, but they are followed only at a project/service level (as needed).

Integrated

Common, aligned OAV management policies are consistently implemented throughout the organisation. Everybody strives to adhere to the defined rules and policies. There is an effort to increase automation of all policies.

Proactive
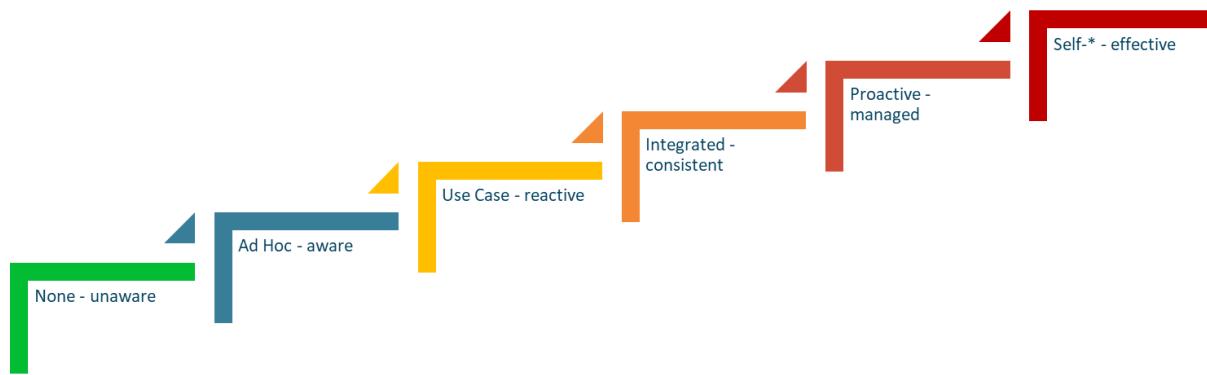
OAV management policies are fully developed, enforced and well-understood throughout the ecosystem. Actions related to necessary policy changes and adaptations are also being automated.

Self-*

OAV management policies are optimised. Controls are implemented in order to ensure that the achieved excellence is sustained regardless of changes in leadership or direction.

3.3.2   Data Governance

Data governance is everything that is done to ensure data is secure, private, accurate, available, and usable. It includes the actions people must take, the processes they must follow, and the technology that supports them throughout the data life cycle [Google Cloud Web]. The MM stages for Data Governance are:

None

There is no information governance in the organisation. All available information is stored in an inconsistent way in various systems managed by different organisation departments or individuals. Data is frequently duplicated and sometimes impossible to join or consolidate because of a lack of proper inter-system references.

Ad Hoc

The organisation is aware of the problem of not having defined data ownership (single source of truth) throughout the departments. At this stage, this problem is addressed at a group/department level only, and not yet at the organisational level. The management understands the need for a consistent information management approach. Departments are becoming aware of problems with data quality as inconsistencies in the stored data are identified.

Reactive

The organisation is able to extract value from the information stored in its systems. Data is shared between systems managed by different departments while retaining a single-source-of-truth approach. Data quality issues are resolved reactively using an organisation-wide approach.

Integrated

The value extracted from consistent data stores is used for decision-making at different management levels. Data owners and data stewards are in charge of ensuring high data quality and standardised data management processes. All data is being governed in a consistent way organisation-wide.

Proactive
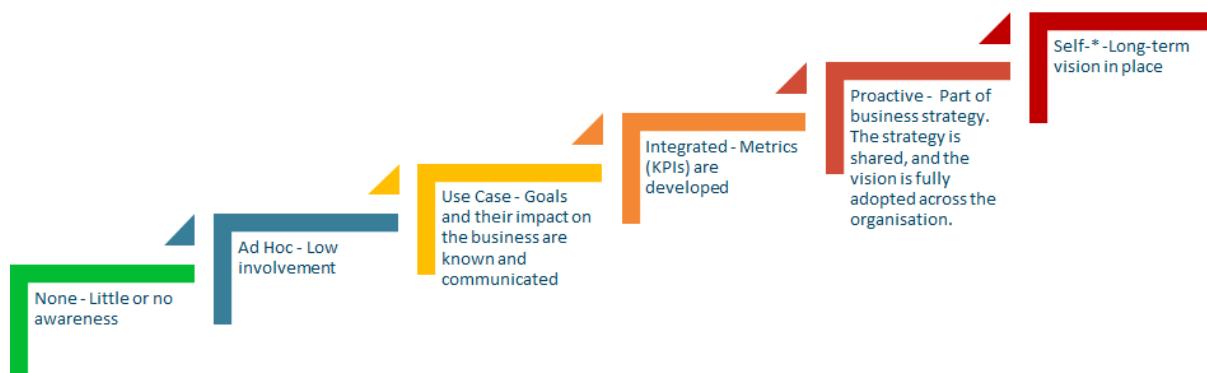
A high-level governance body ensures proper data governance across different departments and standardised data sharing with partners within the ecosystem. Best practices are used consistently throughout the ecosystem. Different metrics are used to identify the success of data governance functions.

Self-*

Information management is considered to be the key ingredient for creating value with efficiency and agility. Data governance is stable and well-defined within the OAV framework, supporting the coordinating efforts within the ecosystem. Information-based strategies are used to minimise risks and enhance effectiveness with the help of AI.

3.3.3   Strategic Approach

A strategy approach is a methodical plan designed to achieve specific long-term goals and objectives. A strategic approach can apply to a variety of topics. In this section, the focus is on the strategic planning of OAV activities, based on the following stages of maturity:

None

In the none stage, there is little or no awareness of strategic planning related to OAV activities. A traditional strategic management style is used where the business side of the organisation is not aware of the networking/IT departments' potential.

Ad Hoc

In this stage, ad-hoc OAV activities are gaining interest, but the overall level of involvement across the organisation is low. The OAV goals are unclear on the business level, and no OAV vision is being developed. There is very limited understanding of the potential of OAV from the business perspective, especially in non-technical departments such as finance or customer relations.

Use Case/Project-Based – Reactive

OAV goals and their impact on the business are known and communicated. A strategic roadmap to OAV enablement is being created and there is an attempt to coordinate efforts, but there is no widespread vision adoption. The business now sees OAV as a potential driver and starts to understand its value, however, this understanding is limited to the management, with no actual alignment between the technical and non-technical departments.

Integrated

A formal OAV development strategic plan is being implemented in a coordinated way so that an innovative approach to OAV is supported across all departments. Metrics (KPIs) are developed to be used as indicators for planning future efforts. The vision is embraced by the cross-functional teams and all non-technical departments begin to understand the OAV strategic plan and their role and expected involvement in the transformational process.

Proactive
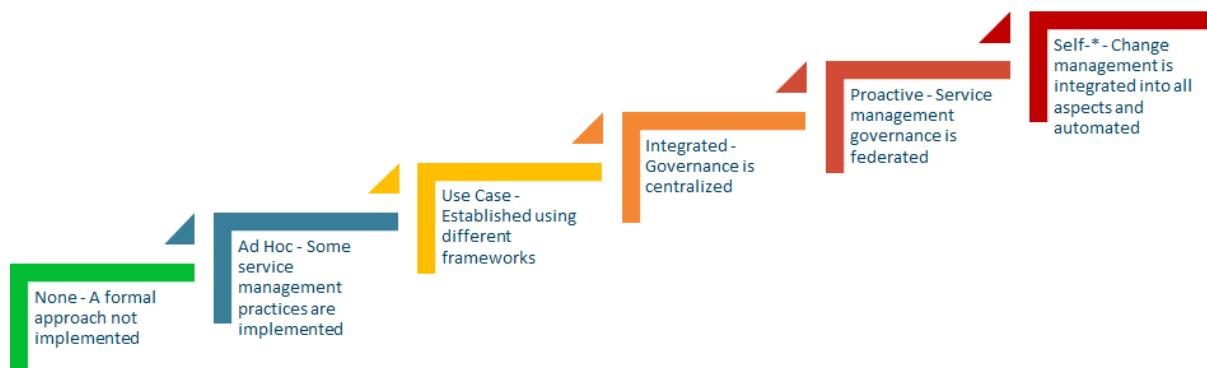
OAV is part of an all-encompassing business strategy and vision development for value creation in the organisation. The strategy is shared, and the vision is fully adopted across the whole organisation. Consistent actions are taken according to the tracked metrics. All employees from both technical and non-technical departments support the OAV vision and are actively involved in its implementation.

Self-*

There is a long-term vision in place focusing on continuous innovation using OAV organisation-wide. The organisation has developed clear strategic alliances and is working on its strategic innovation OAV capacity, aiming to provide value beyond expectations. Business and OAV are fully aligned not just within the organisation, but across the ecosystems of all partners.

3.3.4 Service Management Capability

The stages of maturity of implementation and management of quality IT services that meet the needs of the business can be defined as follows

None

No formal approach to service management is implemented.

Ad Hoc

Some service management practices are implemented in an isolated manner by individual teams/groups with various levels of maturity. Problem and incident management are reactive, and knowledge management is used for incidents only.

Use Case/Project-Based – Reactive

Service management is now being established using different frameworks across teams with different views on practices and their integration. These framework implementations are independently governed and measured. Additional practices are developed for the service catalogue, service level management, change management, change configuration, and request fulfilment.

Integrated

A single service management framework and approach to practices is common across the organisation. All existing management frameworks are now integrated, and problem management is starting to be proactive. Governance is centralised.

Proactive
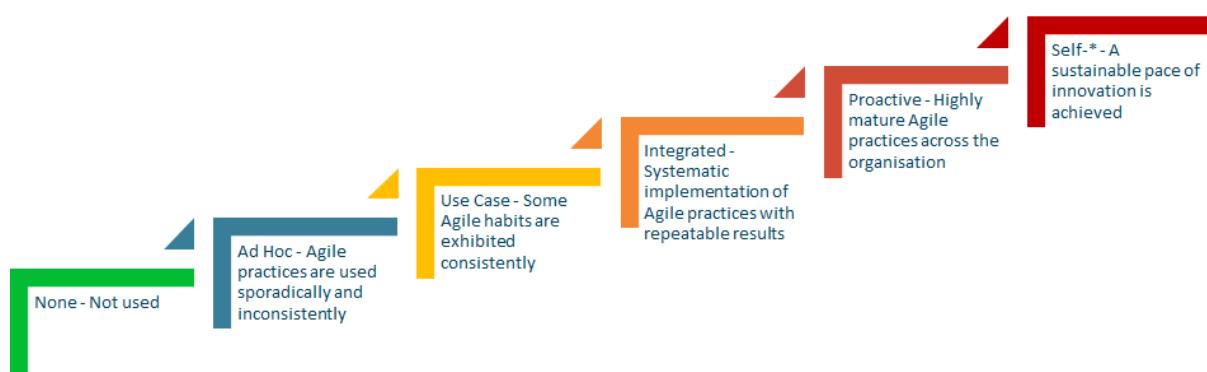
Service management governance is federated. There are automated reports and dashboards across all service management domains. Service management is implemented for bundled multi-domain services.

Self-*

Service management functions with optimised governance and metrics are automated. Change management is integrated in all aspects and automated as much as possible. All mechanisms related to continuous improvement are implemented.

3.3.5   Agility

Agility is the ability to adapt and respond to change [SAFE Web]. The maturity stages of organisations in terms of agility are:

None

Agile practices are not used in any OAV project management and software development efforts in the organisation.

Ad Hoc

Agile practices are used sporadically and inconsistently across the organisation. Work is done with variable quality and there is little cross-project knowledge-sharing and collaboration. Success is achieved through individual efforts.

Use Case/Project-Based – Reactive

Agile practices become common and some agile habits are exhibited consistently. There is variable consistency across teams. Some knowledge-sharing activities are underway. Results greatly improve in quality.

Integrated

The organisation is starting to implement lean portfolio management. Agile characteristics and behaviour mature. There is systematic implementation of agile practices with repeatable results. Appropriate agile governance is in place.

Proactive

Highly mature agile practices are implemented across the organisation. Agile is successfully used at scale with distributed teams. There are measurement systems in place that keep track of business value delivery.

Self-*

Lean and agile are part of the organisational culture. The teams are aiming for perfection in terms of waste reduction, eliminating inefficiency and supporting a smooth delivery flow. A sustainable pace of innovation is achieved. Continuous organisational learning and optimisation permeate all work actions.

3.3.6   Standardisation

Standardisation refers to the establishment of a set of rules governing how a given task or sequence of tasks are completed in an organisation [Process.st]. In terms of OAV maturity, the stages of standardisation are:

None

OAV-related standardisation is not considered.

Ad Hoc

There is little adherence to existing OAV-related standards emerging in some departments and focusing on isolated aspects.

Use Case/Project-Based – Reactive

Some units or departments demonstrate adherence to existing OAV-related standards. A standardisation strategy is being developed.

Integrated

An organisation-wide internal OAV-related standardisation approach is being implemented. Standards are considered in each new undertaking and development. Compliance measures are being put in place so that standards are followed in all stages from design to production.

Proactive

Common standardised OAV approaches at the ecosystem level are adopted. The organisation has standardised all its activities related to external partners. Interoperability, compatibility and openness are recognised as the main requirements for successful collaboration.

Self-*

Proactive improvements are implemented to maintain high-performing standardised OAV approaches that are aligned with innovative business approaches.

3.3.7 Investments

Broadly speaking, an investment is the act of committing capital for an asset or a service, with the expectation of generating future value [Investopedia]. In the OAV MM, it refers to OAV-related investments:

None

OAV-related investment requirements are not considered during capital planning or in other related resource budgeting processes.

Ad Hoc

Ad-hoc individual requests for resources or skills development investments related to OAV are made. No planned capital investments exist.

Use Case/Project-Based – Reactive

Capital planning and investment control recognise the importance of investments in OAV. OAV-related requirements are a part of the regular investment planning and execution cycle.

Integrated

All OAV-related financial implications are considered as high priority and are part of capital planning and investment control. OAV cost benefits are clearly demonstrated and supported.

Proactive

There is flexible capital planning and investment control in place that is directly related to the outputs from OAV activities. Regular updates of planned investments are made based on OAV-supported business drivers.

Self-*

OAV metrics are used to optimise and drive future organisation investments on a large scale. Investment planning is in place to support flexible continuous process improvements of OAV.
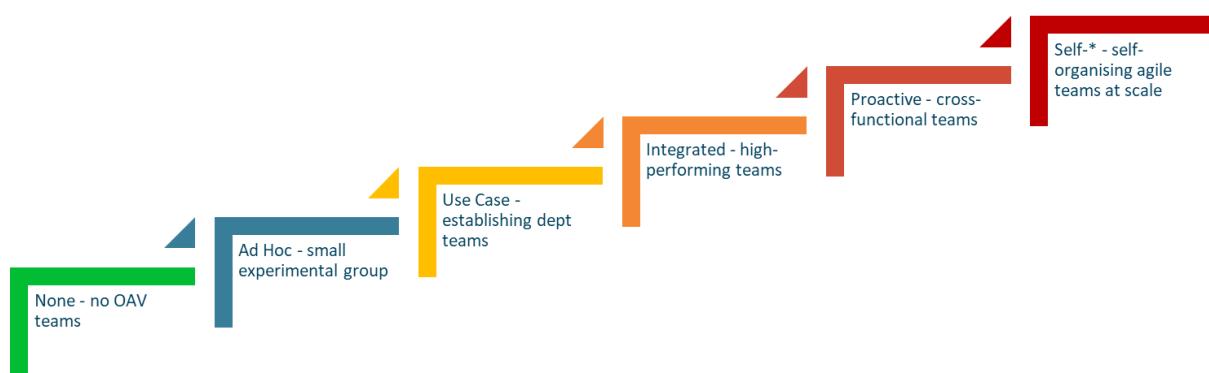
3.4 People and Organisation

This dimension is related to the organisational culture that supports the adoption and advancement of OAV for all stakeholders (internal and external) to achieve an open, innovative, agile and flexible collaboration with partners and users. Related activities include collaboration, organisational structure, talent management, nurturing an OAV mindset, and learning and development of OAV skills – as well as leadership that supports OAV values and helps keep the organisation focused on its objectives.

This dimension is divided into five subdimensions: team, stakeholders, building OAV skills, culture and user/customer experience.

3.4.1 Team

A team is a group of people who perform interdependent tasks to work toward accomplishing a common mission or specific objective. This sub-dimension of the maturity model looks at whether dedicated teams are in place within an organisation to work on OAV capabilities,   and how they are structured, according to the following stages [asq.org]:

None

There are no teams working on OAV capabilities. Only sporadic efforts by individuals who are interested in employing OAV techniques may be noted.

Ad Hoc

Initial small OAV groups are spontaneously formed based on common interests or goals. Any communication, knowledge-exchange and joint development efforts are on-demand.

Use Case/Project-Based – Reactive

Official OAV teams are being formed. A team management structure is being defined and team rules are established. Communication and joint development mainly take place at a department level.

Integrated

Well-established OAV teams are defined within the organisation, focusing on different aspects of the OAV architecture. There is open, trusted communication and collaboration between   all OAV-related teams in the organisation.

Proactive
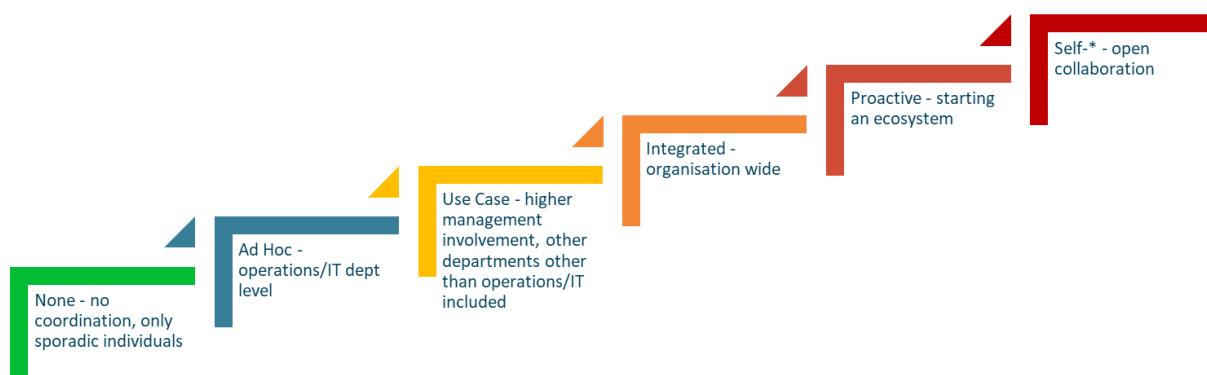
The organisation's teams have evolved into multidisciplinary, cross-functional teams that have a holistic approach to their OAV work. Open, cross-team communication and cooperation on OAV are established within the organisation and across the ecosystem.

Self-*

Self-organising agile teams are established based on the identified objectives and their results are continuously tracked at the ecosystem level. The ecosystem coordinates a team of teams that work on multiple projects that have a common set of objectives (i.e. joint service development).

3.4.2   Stakeholders

Stakeholders are parties that have an interest in a company and can either affect or be affected by the business. They may be internal or external (including individuals and groups outside of the organisation) [Investopedia]. The stages of stakeholder involvement in OAV are:

None

A handful of engineers who may or may not work together in the same department are interested in implementing OAV. There is no coordination between any stakeholders that are interested in OAV, either internally or externally.

Ad Hoc

OAV becomes the topic of discussion at a departmental level in operations and/or IT. The potential benefits and possible routes for implementation are considered by selected department members. There is no coordination with individuals and groups outside the organisation.

Use Case/Project-Based – Reactive

Higher-level management becomes involved, recognising the strategic potential of OAV within the organisation. Attention is given to getting all internal key stakeholders that are directly involved in the implementation of OAV on board.

Integrated

OAV has been successfully adopted by the whole organisation including the management and all departments. Collaboration with experts external to the organisation is initiated where necessary. OAV user requirements are considered as the organisation moves to a customer-centric approach.

Proactive

Partner organisations actively participate in OAV and are recognised as key stakeholders, as OAV provides the means to build a flexible dynamic ecosystem that can support the user requirements for multi-domain bundled services.

Self-*

Using openness as a principle in advancing OAV, the organisation fully engages in collaboration with external stakeholders on various OAV topics (design of new services, extending the user base, etc.).

3.4.3   Building OAV Skills

Skills are the knowledge, expertise, talent, and understanding needed to do a job or task [yourdictionary.com]. The maturity stages as they apply to OAV skills are:

None

There are no envisioned opportunities for learning and building OAV skills in the organisation. Only sporadic OAV learning and skills development efforts exist on an individual basis with unpredictable results. There is only traditional network management expertise available in the organisation.

Ad Hoc

Most efforts are still on the level of self-upskilling. As a result, the first individuals skilled in OAV are emerging and are driving an increasing demand for OAV training. Learning needs are being recognised by the organisation.

Use Case/Project-Based – Reactive

A formal OAV training programme is established and structured programmes for upskilling and expertise development are available. The organisation is investing in upskilling its staff, recognising the value of having

OAV knowledge. "Unicorns" (engineers with knowledge in network technologies as well as DevOps and OAV) showcase the potential of building OAV expertise.

Integrated

OAV skills are considered essential in the organisation and there is a well-defined programme for continuous learning and upgrading. An effective internal talent management approach is employed to guarantee successful talent acquisition and development.

Proactive

An effective talent management approach is adopted that supports OAV talent acquisition and development across the ecosystem. There is a joint effort in upskilling and expertise building between partners in the ecosystem.

Self-*

All upskilling and talent management efforts are fully aligned with the organisation and ecosystem business drivers. Training programmes are optimised according to innovation requirements and long-term strategies.

3.4.4 Culture

In this context, culture includes rules, values, beliefs, and philosophies that dictate team members' behaviour in a company [teambuilding.com]. The stages of cultural maturity for OAV are:

None

The organisational culture is aligned with the traditional architecture and approaches. OAV is considered to be something new, not to be trusted or embraced.

Ad Hoc

The benefits of OAV implementation are being recognised by individuals within the organisation. OAV is considered a prospective change that might be implemented. However, there are no efforts to change the traditional mindset. There is little to no trust in OAV-based methods and tools.

Use Case/Project-Based – Reactive

OAV is beginning to be embraced by teams that have changed their internal culture to adopt it and fully trust the automated processes and related tools. The benefits of OAV are clear, but there are still traditionalists who do not adopt any new initiatives.

Integrated

Trust in OAV and its implementation is spreading organisation-wide. Everyone is on board with the changes brought in by OAV adoption and focused on the related benefits. There is a clear shared effort to replace the traditional mindset.

Proactive

OAV is the new philosophy and everybody uses it for everything. OAV approaches are proposed in all projects and development and implementation efforts by all parties involved. Openness and collaboration are adopted as shared goals in the organisational culture. An agile, flexible portfolio is recognised as a must-have feature.

Self-*

There is deep trust and open collaboration regarding OAV not only within the organisation but also extended externally to all stakeholders in the ecosystem. Motivation and enthusiasm are carefully nurtured so that everyone is aware that they can make a meaningful impact through effective collaboration and progressive development. OAV innovation and continuous improvement are fully coordinated in the ecosystem.

3.4.5 User/Customer Experience

User/customer experience is the overall perception and impression a user/customer has of a brand or company based on their interactions and experiences across various touchpoints. It encompasses all interactions, from initial awareness and engagement to purchase and ongoing support, and includes factors such as customer service, product quality, convenience, and the emotional connection between the customer and the brand. The stages of OAV user/customer experience are:

None

The organisation uses traditional channels to communicate with its customers. All communication is mainly initiated as a response to a user inquiry using a manual approach. There is no feedback gathering for the purposes of improvement.

Ad Hoc

The information flow is improved so that users can be (semi)automatically redirected to a team that can answer their questions or fulfil their requests thus reducing response time. New communication channels such as simple bots are starting to emerge. Customer feedback is starting to be gathered.

Use Case/Project-Based – Reactive

The organisation is invested in the customer experience. Customer engagement is partially proactive where users are contacted in advance to inform them about any actions that might impact their experience (to be able to do this the organisation must be able to automatically answer questions such as "Which users are going to be impacted by this action?"). Regular feedback gathering is in place.

Integrated

The organisation is using its connected OAV systems and unified automated processes to heighten the customer experience. The customer experience is improved by making all standard actions easy to request and fast to fulfil with minimum human intervention, for example, automated registration or personalised content recommendations.

Proactive

Digital presence with cross-channel capability is provided to users using automated context switching and intelligent suggestions. The organisation is capable of a 360-degree customer view by combining the data from different functional OAV components thus creating a full image of the user and their history. Customer experience is the main driver for all organisational strategic decisions.

Self-*

The organisation exhibits omni-channel capabilities where the user context can be seamlessly switched between communication channels. Customer self-actions are available for all users with the goal being zero personal contact using integrated and smart OAV systems.

4 Conclusions

The maturity model described above was developed for the research and education community to take into account the differing Orchestration, Automation and Virtualisation (OAV) adoption levels found within different NRENs and the importance of this topic for the community in the long term. However, its applicability extends to any individuals or groups with a specific interest in OAV. Its primary purpose is to serve as a self-assessment tool in these domains. It may also serve as a set of recommendations on how the different areas considered in this model, referred to as "dimensions" (Architecture and Technology, Processes and Services, Vision and Strategy and People and Organisations), can be evolved step by step and bring all aspects of communication processing into an integrated and smart OAV system.

The maturity model, together with the materials developed by the Network eAcademy (OAV training, Terminology document, Architecture Mapping, Wiki) aim to assist organisations to better manage and accelerate OAV adoption in their path towards digital transformation. By periodically taking the OAV MM survey, NRENs can assess and track their OAV evolution against the average for the community. The maturity model report also identifies dependencies and areas where they can progress or where process duplication occurs and offers valuable insights into potential subsequent actions that an organisation can take to advance towards more integrated systems.

The flexibility of the model, with its dimensions and subdimensions, also allows a fine-grained evaluation which is especially important in the highly diverse research and education community, where no one system fits all. This also means that each research and education organisation can use the model as needed or when new developments have been applied and explored, as a tool to achieve optimisation towards more integrated and smarter OAV systems – even if the organisation's requirements do not demand fully fledged Self*- capabilities.

The OAV Maturity Model additionally enables organisations to compare their current status with that of other organisations that have previously responded to the survey – focusing on trends and the individual organisation's position within those trends. It can also help highlight in which areas expertise already exists in the community, or where conversely skills-building activities would be welcome to support organisations towards achieving higher, more advanced stages of OAV maturity.

References

[GN4-3_D6.2]	https://resources.geant.org/wp-content/uploads/2022/02/D6-2_Automation-and-Orchestration-of-Services-in-the-GEANT-Community.pdf
[Maturity Model 1]	The maturity model for Network & Infrastructure Management. (n.d.).
[Maturity Model 2]	A maturity model for assessing the use of ICT in school education. Educational Technology and Society, 16(1), 206–218.
[Solar, M., Sabattin, J., & Parada, V. (2013).]	A maturity model for assessing the use of ICT in school education. Educational Technology and Society, 16(1), 206–218.
[Bass, J. M. (2011).]	An Early-Stage ICT Maturity Model derived from Ethiopian education institutions. International Journal of Education and Development Using Information and Communication Technology, 7(1), 5–25. http://0-ijedict.dec.uwi.edu.innopac.up.ac.za/viewissue.php?id=28
[Haris, F. (2010).]	IT Infrastructure Maturity Model (ITI-MM) A Roadmap to Agile IT Infrastructure. 118.
[Pham, Q. T. (2017).]	Measuring the ICT maturity of SMEs. A Knowledge Management Approach for Ensuring the Success of IT Industries in Vietnam, January 2010, 1–24.
[De Sousa Pereira, R. F., & Da Silva, M. M. (2010).]	A maturity model for implementing ITIL v3. Proceedings - 2010 6th World Congress on Services, Services-1 2010, 399–406. https://doi.org/10.1109/SERVICES.2010.80
[Proenca, D. (2016).]	Methods and techniques for maturity assessment. Iberian Conference on Information Systems and Technologies, CISTI, 2016-July. https://doi.org/10.1109/CISTI.2016.7521483
[OAV MM Survey]	https://www.surveymonkey.com/r/SPYDQVB
[NA_eAcademy]	https://connect.geant.org/2021/10/27/network-automation-eacademy
[Rathfelder, C., & Groenda, H. (2008).]	An independent SOA maturity model. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5053 LNCS, 1–15. https://doi.org/10.1007/978-3-540-68642-2_1
[Net, T. (1998).]	The Network Maturity Model for Internet. 910, 117–118.
[Cisco Web]	What Is IT Security: https://www.cisco.com/c/en/us/products/security/what-is-it-security.html
[SAP Web]	What is analytics: https://www.sap.com/products/technology-platform/cloud-analytics/what-is-analytics.html
[Data Definition]	Data meaning: https://www.oed.com/
[The Tech Edvocate]	What is Service Life Cycle Management (SLM): https://www.thetechedvocate.org/what-is-service-life-cycle-management-slm/
[SIG-NOC Tools Survey]	Monitoring and reporting definition: https://wiki.geant.org/display/SIGNOC/SIG-NOC+Tools+Survey+2019
[IBM Web]	Introduction to troubleshooting: https://www.ibm.com/docs/en/om-jvm/5.4.0?topic=support-introduction-troubleshooting
[ITIL]	Security management definition
[Google Cloud Web]	What is Data Governance: https://cloud.google.com/learn/what-is-data-governance
[SAFE Web]	Organisational Agility: https://scaledagileframework.com/organizational-agility/

[Process.st]	Why Process Standardization Improves Quality, Productivity, and Morale: https://www.process.st/process-standardization/
[Canara HSBC]	What is Investment: https://www.canarahsbclife.com/blog/financial-planning/what-is-investment
[asq.org]	What is a Team: https://asq.org/quality-resources/teams
[Investopedia]	What Are Stakeholders: Definition, Types, and Examples: https://www.investopedia.com/terms/s/stakeholder.asp
[yourdictionary.com]	Examples of Skills: Job, Life, and Personal Skills: https://www.yourdictionary.com/articles/examples-skills-list
[teambuilding.com]	Organisational Culture: Definition, Examples, & Best Practices: https://teambuilding.com/blog/organizational-culture

Glossary

AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
CFS	Customer Facing Services
CLI	Command Line Interface
DevOps	Development and Operations
ETL	Extract, Transform, Load
GUI	Graphical User Interface
IDS	Intrusion Detection System
IOA	Indicators of Attack
IOC	Indicators of Compromise
IPS	Intrusion Prevention System
IT	Information Technology
KPI	Key Performance Indicator
ML	Machine Learning
NFV	Network Functions Virtualization
NREN	National Research and Education Network
OAV	Orchestration, Automation and Virtualisation
R&E	Research and Education
REST	Representational state transfer
RFS	Resource Facing Services
SIEM	Security Information and Event Management
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
TTP	Tactics, Techniques, and Procedures
VM	Virtual Machine
VNF	Virtual Network Function
VPN	Virtual Private Network
XML	eXtensible Markup Language
YANG	Yet Another Next Generation