Efficient Hybrid IT Operations for SAP® Customers
How to Govern the Operation of Hybrid Landscapes
Getting It Right

It is crucial to have full transparency on all cloud providers delivery according to agreed service levels such as availability, performance, and initial time of response for a disruption.

When moving to hybrid landscape, a successful hybrid IT operations and service management requires a business process and object-oriented IT service management. The definition and the orchestration of end-to-end services become key for the success of operating hybrid landscapes.

You must have clear transparency of the status of all service requests raised.

The capability to measure the service levels end-to-end is very important. You need tools to measure the service provider effectively, ensuring both the contractual compliancy and non-contractual obligations. The precise definition of metrics and KPIs is important which should also be aligned and agreed from business to IT, from IT to cloud service providers and from IT to partners. This alignment gives you the necessary trust and confidence that hybrid solutions provides a level of service to the full satisfaction of your business.

It also enables your IT to have the capability to act as single contracting partner for your business.
MANAGING INCIDENTS

Enhancing the landscape by SaaS solution
The formal description of ITIL for incident and problem management is to restore a normal service operation as quickly as possible and to minimize the impact on business operations. But in a hybrid landscape it needs adoption due to the higher distribution of responsibilities. The end users on the other side are no longer aware of the technology or systems used in the background and this has major implications on the incident and problem resolution.

The cloud provider’s incident management systems are designed and used to report issues to your cloud service provider. There is effectively a gap in your ability to govern your incident management if users directly report incidents to your SaaS provider and not to you. If an incident requires a development from the cloud service provider, these development requests are often captured in a separate tool, often with no transparency about status and progress of the bug fix development for you.

With the move of certain business activities to cloud based solutions your IT no longer needs to monitor some operations, except for things like insufficient hardware resource consumption or degrading performance of solutions. Alerts or events along the technology stack are usually not made transparent to your people. The SaaS service providers supporting tools and infrastructure is in most cases not in your sphere of influence. The overall service level measurement should address your reporting needs and are usually provided by self-service to you without any further integration capability to your dashboards or operations tools. That’s why SAP provides access to SAP Trust Center, Cloud Availability Center, and SAP ONE Support Launchpad.

Your responsibility for support, operations and incident management stays for the on-premise component, the application layer for PaaS components and of course for the complete integration layer including all aspects of interface management, data consistency management, and business application management.

An end-to-end view on aspects like landscape health or business process health is usually not available out of the box for all components of the hybrid landscape.

As the business solution is deployed over cloud and on-premise solutions, integration, and orchestration of various teams to effectively manage and safeguard critical events and incidents across the complete application landscape is required. In case of a business process interruption transparency on the flow of the business steps across the different technical solution components with different deployment models across the hybrid landscape is key to understand the impact and to solve an incident.

Figure 12: Dashboards of SAP Trust Center, Cloud Availability Center, and the SAP ONE Support Launchpad.
MANAGE THE HYBRID LIFECYCLE

On-premise only situation
In an on-premise only landscape, your IT team is fully responsible for release management including the planning, scheduling, and control of the deployments. In any deployment, you have complete control and transparency of all release phases and the release components in the process. Your IT operation team is completely responsible and accountable for defining the release strategy. This includes, for example:

- The frequency of releases
- Scoping of release components
- Definition of release and downtime windows
- Enterprise upgrade strategies and planning

Having control and the transparency on the release phases along with the proper use of service management tools enables IT operations to effectively govern the release management processes. Controlling the deployment of the different release components allows IT operations to plan and test effectively in the release cycle regardless of the ownership of the different aspects of the solution.

Enhancing the landscape with an SaaS solution
Change and release management is impacted by the hybrid infrastructure itself. This requires the adoption of those processes in different dimensions. You need to distinguish between releases and changes delivered by the solution provider in the sense of patches or feature extensions or customer raised releases or changes as a result of customer owned or customer requested development.

When moving to a hybrid landscape, you might be governed and limited by the release strategy of the cloud providers, reducing the flexibility for ad-hoc changes. Here is a comparison of the current release shipment strategy in on-premise and cloud-based worlds. The challenge in a hybrid landscape is to combine both.

Figure 13: Nonaligned releases between cloud and on-premise solutions
Different SaaS providers deploy periodic releases for either standard new functionality or upgrades to their infrastructure. SaaS solutions impose new types of change events to hybrid solutions. At given release dates the SaaS provider deploys UI and feature updates, bug fixes or opt-in changes where you can select new cloud features.

SaaS products can impose changes to your change and release strategy. The alignment of your release strategy with the release strategy of the SaaS providers is a challenge, as the cloud provider cannot adapt their release strategy serving thousands of customers. As a consequence, customers are forced to synchronize their releases with the cloud provider releases.

The level of execution related to SaaS product is greatly reduced as this now falls in the domain and responsibility of the cloud provider. For the cloud component the SaaS provider focuses on the aspects of planning, orchestration, monitoring, and decision making in their release processes, while your IT operations is fully responsible for all aspects of the integration to the on-premise parts of any software solution.

Your IT needs to have the capability to estimate the impact of any the change imposed by the release cycle of the SaaS solutions to their overall hybrid business solution. Different roles with a strong architectural and functional domain and/or industry understanding are needed to evaluate the impact of any type of (cloud) change before it reaches the productive landscape. You are responsible for validating the solution provided by the cloud provider and are fully responsible for all integration aspects to the on-premise part of the software solution.
TESTING IN HYBRID LANDSCAPES

It is a common misperception that there is no need for testing in hybrid environment. This statement is partially true for a cloud only deployment when the SaaS provider deploys so-called universal changes. A universal change is an update where the SaaS provider provides UI and feature updates, and/or bug fixes. In this case customers expect not to test at all. The same is valid for new releases, where new content and features are provided by the SaaS provider.

In a cloud only environment customers do not expect to test intensively, nevertheless, there is still a need for user acceptance test (UAT) in a cloud only deployment. During UAT, actual users test the software to make sure it can handle required tasks in real-world scenarios. UATs in cloud only deployment are usually required after the initial set up, or in case that the business chooses to use newly available feature (opt-in). If the customer decides to use additional business processes provided by the SaaS software UATs are also required.

When introducing cloud extensions or on-premise elements to the cloud solution the test requirements for mission critical business processes spanning over the now hybrid landscape increases drastically. The need for functional integration test and regression test for mission critical processes are almost the same as in a on-premise only word. This is necessary as in most cases the on-premise solution standard is to some extend modified. Therefore, functional integration testing, in which individual software modules are combined and tested as a group, are becoming necessary when the customer first is going live with his new hybrid landscape.

Later in the life cycle when customers are doing an opt-in on the SaaS component or activates new business process scenarios functional integration tests are recommended.

For all cloud triggered change events regression tests are recommended for all mission critical processes that are spanning over the hybrid solution. Regression tests ensure that previously developed and tested software still performs the same way after a change.

Cloud extensions developed on SAP Cloud Platform should be handled from quality management and test management perspective in the same way as customer code or modification in an on-premise environment.

SAP Cloud Platform also gives you the opportunity to apply DevOps (Development Operations) principles. DevOps is a combination of development and operations capabilities, operating together with common goals and objectives that facilitate the adoption of continuous integration (CI) and continuous delivery (CD) development practices, with emphasis on continuous process improvement. DevOps is not a methodology nor a framework, it is a culture, a movement, a philosophy built on the four principles of culture, automation, measurement, and sharing. Instead of shipping large releases, smaller packages are shipped more often.
Customer’s IT responsibility for hybrid Integration
Even though the SaaS applications integrated to the hybrid landscape are used in a fairly standardized way, the end-to-end business scenarios spanning over the different deployment models are always customer specific. The reasons for complexity in hybrid landscapes is in general introduced by non-SaaS components that are often highly modified from the standard. Often data models or standard business processes in the on-premise system have been modified and are different from the models used in the cloud solution.

For the technical integration of cloud with non-cloud components SAP offers a wide range of methods and technologies. For example, the integration of SAP ERP on-premise systems and SAP Ariba is supported by four different integration technologies: APIs, SAP Cloud Platform Integration, SAP Process Integration and direct web services between SAP ERP and SAP Ariba. This results into a federated integration architecture involving multiple SAP and non-SAP tools and methods in one individual hybrid scenario.

On the one hand, business expects that IT ensures business continuity regardless the end-to-end deployment scenario, while on the other hand there is not one party that owns and controls IT operations from an end-to-end perspective in a hybrid landscape. Often there is an expectation that the SaaS provider should take care of managing the cloud integration. In fact, it is the customer’s IT responsibility to fully integrate all scenarios and to ensure the business can use the end-to-end solution to run the core processes. Managing the cloud integration in the aspects of managing all types of exception along the hybrid deployment, managing the consistency of data and doing the integration monitoring are the essential customer IT responsibility.

One place to manage all exceptions
Another complexity of integrating SAP cloud solutions is the fact that you may not be using just one monitoring tool in your IT estate.

Quite a significant number of customers do NOT use ONE central tool for their technical operations. Different tools for job management, technical monitoring beyond SAP Solution Manager being used in one solution landscape at the same point of time are common.

Customers have already challenges to bring alerts, incidents and exceptions in their on-premise estate from different tools into one platform/inbox from where they can process them centrally. Using multiple set of tools for operations and monitoring is becoming challenging with a large manual consolidation effort. On top of it some customers manage cloud exceptions from different consoles and places.

In order to manage the exceptions along a business process that is spanning over a hybrid landscape, you need one central place to manage alerts and exceptions regardless where they originated from. You need end-to-end view to govern all relevant operations aspects.