1.

Guide

Hybrid Operation

Operating Concepts for SAP Solutions

Version 2021

Authors

Name	First Name	Company	E-Mail Address
Berhorst	Ralf	Miele & Cie. KG	ralf.berhorst@miele.com
Dürk	Marc-Oliver	SAP SE	m.duerk@sap.com
Hauzeneder	Constantin	Rohde & Schwarz GmbH & Co. KG	Constantin.Hauzeneder@rohde-schwarz.com
Sperzel	Sabine	Evonik Industries AG	sabine.sperzel@evonik.com
Wagner	Philipp	Getinge Deutschland GmbH	philipp.wagner@getinge.com
Zimmermann	Ronny	University of Magdeburg	ronny.zimmermann@ucc.ovgu.de

Table of Contents

List of Figures

List of Tables

Topic Areas

1 Introduction/Model Company

Many companies are faced with the challenge of adding new cloud technologies to their existing on-premise landscapes. The purpose of this guide is to assist IT Basis staff involved in supporting companies that are transitioning towards this kind of hybrid system landscape. It is based on best practices from various companies that have been collated since 2017 as part of the DSAG project “Operating Hybrid Landscapes”. This is the successor to the “SAP Basis of Tomorrow” project, which was also dedicated to exploring future demands on IT basis departments.

It’s important to make it clear from the start that there is no single correct approach or ideal structure for a hybrid landscape. Every company’s individual IT landscape is unique and is the result of the company’s particular business activities and of decisions that have been made along the way. We would however like to raise awareness of potential problems that commonly arise when operating hybrid landscapes and to refer to the tools provided by SAP for these situations.

Joe's Fidget Spinners Inc – The Model Company for Hybrid Operation

A hybrid landscape comprises multiple cloud solutions (IaaS, PaaS, SaaS) and on-premise systems. To illustrate the working of this system landscape, allow us to introduce the toy manufacturer Joe’s Fidget Spinners Inc, a company which operates precisely this kind of hybrid landscape:

Joe’s Fidget Spinners Inc has been a successful company for a number of years. Rapid growth and new technologies have made changes to the business model and a transformation of the IT landscape necessary.

- The business would like to transform its sales setup, thus far made up exclusively of sales representatives, by introducing a global end-customer direct sales solution in the form of a web shop. This should make it possible for customers to customize products (lot size 1) and to keep track of the status of their orders. In order to take account of security considerations and global availability, the company has decided against implementing the services required in their own data center in favor of a Platform as a Service solution in the cloud.

- Various LOBs are dissatisfied with the rate at which IT projects are implemented, especially in cases where services are to be provided both internally and externally. In order to further guarantee the stability of the core systems (digital core) while enabling faster development with non-critical/agile systems, companies have ceased programming certain developments and enhancements on internal systems in favor of using *Platform as a Service* offerings as their development and runtime environment.
- The IT department seeks to make better use of its hardware and software resources and would like to see peaks arising during projects represented as opex (operating costs) rather than capex (capital expenditure). Resources for systems that are only used temporarily should therefore be rented from an *Infrastructure as a Service* provider.

For some years now, Joe‘s Fidget Spinners Inc has been running SAP as its central ERP system, which has enabled its IT organization to acquire a corresponding level of expertise. Given the company’s long-standing membership of the DSAG, its colleagues always keep abreast of the latest trends and developments at SAP. The SAP Basis team at Joe‘s Fidget Spinners Inc were particularly impressed by the DSAG Guide “SAP Basis of Tomorrow”. After performing an in-depth analysis of the current situation at Joe‘s Fidget Spinners Inc, the board realized that, far from making operations leaner, transitioning towards a hybrid solution actually makes things more complex.

Today, Joe‘s Fidget Spinners Inc runs a hybrid landscape, comprising the following systems and applications, operated either in their own data centers or acquired from SAP in the form of a cloud solution or platform.

Joe‘s Fidget Spinners Inc runs the following on-premise SAP systems:

- SAP S/4HANA – in line with the company strategy, the digital core for core business processes remains on-premise.
- SAP BW – the analysis environment receives data from a central system and provides all of the company’s reporting.
- SAP PO – as the company has to serve a series of different interfaces, the SAP PO system is used as the central “data hub”. The same applies for the exchange of data with applications and services from the cloud.
- SAP Solution Manager – a central tool for managing the SAP system landscape, both technically (monitoring, service desk and so on) and at application level (solution documentation, test management and so on).
- SAP Landscape Management (SAP LaMa) – used by SAP Basis for technical control of the system landscape, and performs important tasks, such as system copies.
- MES (non-SAP) – a manufacturing execution system is used to connect the company’s own production and production system to the central ERP.

- SAP Cloud Connector – provides the technical component for connecting on-premise systems with SAP Cloud Platform.

Joe's Fidget Spinners Inc runs the following cloud applications and platforms:

- SAP Cloud Platform – the webshop for global direct sales is developed as an application on SAP Cloud Platform.
- SAP Cloud Platform Integration Service – as the counterpart to the on-premise data hub PO, this connects the on-premise systems with the cloud applications.
- Cloud for Customers – all sales processes for sales representatives are represented via this SaaS solution.
- IaaS Public Cloud – in projects that require the temporary provision of sandboxes, PoCs, and training systems, the company employs the resources of an IaaS provider.

The figure below illustrates the system landscape:

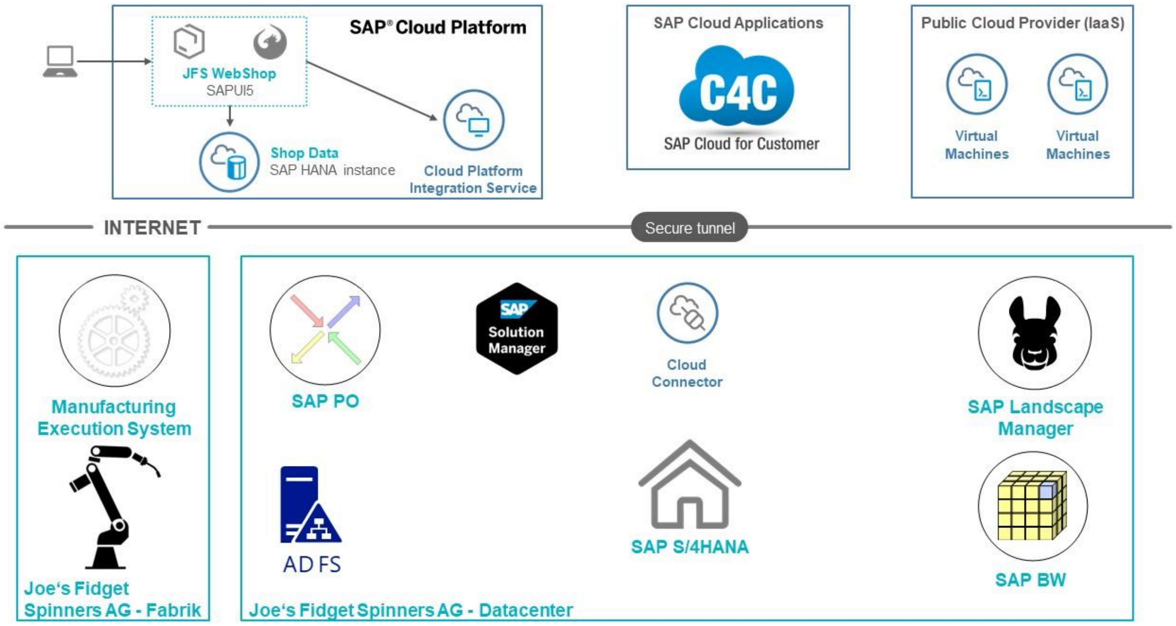

Figure 1: Cloud Applications and Platforms at Joe's Fidget Spinners Inc

2 Definition of Terms

We distinguish between the following types of landscape[1]:

- On-Premise Landscape: No cloud solutions are used
- Hybrid Cloud: No on-premise systems are used; various cloud deployment models are used (IaaS, PaaS, SaaS)
- Hybrid Landscape: On-premise systems and cloud solutions are used

Deployment Models and Examples:

- On-Premise: Software installed at the customer, SAP ERP for example
- Private Cloud: Software operated by the customer in their cloud infrastructure
- Managed Private Cloud: Software/systems in the cloud, which are directly assigned to the customer (such as SAP HANA Enterprise Cloud).
- Infrastructure-as-a-Service (IaaS) Cloud: A cloud infrastructure that is hired from a provider and can be installed and operated on the company's own software (AWS for example)
- Platform as a Service (PaaS) Cloud: A runtime and development environment with additional services, where customers develop and operate their own software (such as SAP Cloud Platform)
- Software as a Service (SaaS) Cloud: Software is offered and operated by a third-party provider for use by the customer (SAP SuccessFactors for example).

3 Discovery & Cloud Onboarding/Offboarding

This chapter is intended as a checklist for cloud onboarding. To begin with, we recommend establishing a cloud onboarding team dedicated to dealing with questions right from the procurement process in order to recognize dependencies at an early stage. We also provide a technical checklist for the onboarding team.

3.1 Cloud Onboarding Team

- Basis staff: For technical details, the technical assessment, service catalog, ITSM and so on, we recommend outlining a sketch of the current landscape.
- Infrastructure staff: Responsible for IDM, networks and so on.

[1] A helpful overview of the various deployment models and SAP offerings can be found at https://support.sap.com/en/tools/software-logistics-tools/landscape-management-process.html#panel-section-accordion-accordionitem-body.

- Governance/Security staff: Responsible for clarifying data protection issues, release clauses and security-related questions.
- LOB: Will the new software meet the business requirements of the users?
- Purchasing: Sets the conditions for initial use as well as for potential further purchases for other users. Offboarding conditions can also be agreed upon if necessary.
- Developers: Can ask detailed questions about the potential solution's enhancement concept. Is it possible to tailor the solution to the company?

In a Software as a Service solution, the infrastructure level normally cannot be influenced by the customer and is therefore not important. It is recommended however to acquire an understanding of the maintenance processes. In the case of maintenance processes effected by the provider (such as updates), the user solution can react in various ways. This should be taken into account when defining the test scenarios. The technical colleagues (Basis) should also check and test the entire process, from problems arising for end users, through creation of tickets for these problems, to forwarding of the tickets and provision of solutions by the cloud provider. When Basis activities like these are outsourced, there is an increased risk of internal technical expertise being lost. In situations like this it can sometimes be necessary to call upon an external service provider to perform the technical assessment.

It is particularly important to pay attention to the responsibilities and to check the high-availability concept and SAP's service agreement. The support models have to be adapted to the existing on-premise agreement, since the cloud solutions are not automatically aligned with it. Services that are covered at present might have to be posted separately for the cloud.[2]

3.2 Technical Checklist

3.2.1 Service Level Agreements

When drawing up the service level agreement (SLA), the solution and the company's business model both have to be considered. We strongly recommend having close alignment between the responsible department and the IT team in order to take account of in-house operational level agreements, such as infrastructure services.

It is absolutely necessary for the responsibilities for the supply model to be defined unambiguously in a jointly agreed service catalog. The basic principles are generally set out in the agreements or statements of work. This must include a precise agreement on the required operation and maintenance processes that can provide the

[2] 07-2019: https://support.sap.com/en/offerings-programs.html#section_792055716

basis for the practical work, and prevent delays further down the line when operation has started.

The service level agreements should also incorporate definition of the general conditions in the form of service parameters. SLAs are often reduced to mere availability SLAs, although this is not sufficient for analyzing the quality of service. We recommend precise definition of the measurement algorithm for the parameters. It can be helpful for example to agree on specific response time SLAs in accordance with the processes (SAP Batch, Online or RFC for example) or E2E SLAs in different regions. An overview of the service parameters is provided in theSAP Basis Operation.

3.2.2 Security Assessment & Data Ownership

When introducing software, a Security Assessment should generally be carried out in order to build fully secure landscapes (security by design). This involves checking the certification status of the cloud solution and of all integration components, also with regard to SOC2 reports. If specific requirements apply (in the automobile sector or in medical technology for example), the company's internal compliance requirements have to be checked (see Security).

3.2.3 Check the Solution's Data Protection

It is also necessary to check whether all legal prerequisites are met (where is data stored, who can view it, privacy shield agreement and so on). It should be noted here that it can take **several weeks to perform a legal check**.

3.2.4 Data Migration/Data Sync/Data Integration

Migration of master data and transaction data is a core part of the onboarding process. The exchange of data, the technology to be used, and the mapping, should therefore be clarified at an early stage. Mapping the data structures can be particularly time consuming. It is also necessary to take account of legal requirements: Which countries have specific data storage legislation? (USA/GER, RUS/GER for example). This has to be taken care of by the governance team (see Integration).

3.2.5 User Management

A new cloud solution is very unlikely to be compatible with the existing user management of the on-premise systems. The following questions therefore have to be examined together with the responsible LOB and the governance team:

- Who is an administrator?
- How are authorizations assigned in the new solution?
- Is there a connection to the existing IDM?
- How is access management regulated?
- Who will be responsible for provisioning authorizations and how?
- Are there existing naming concepts that need to have cloud themes added to them? All cloud users start with a fixed prefix followed by a number for example.
- Is deprovisioning taken into account

3.2.6 Check Integration Capacity

Master data, transaction data, SSO, SAML, IDM, ticket connection and so on must all be taken into account during integration. During the implementation of a cloud solution, it is surprising how little attention the sales team and the line of business often pay to the technical setup, and to what extent they underestimate the question of connecting the cloud solution. The internal IT team can quickly find itself on the defensive here if the cloud sales team underestimates the task of closing the deal quickly. Only the internal IT team is cognizant of the prerequisites and governance regulations (legal) in their company. It is therefore essential for the SAP Basis team to be involved in the selection process.

3.2.7 Architecture

All interfaces between the existing on-premise landscape and the new cloud solutions must be described clearly as a way of preparing integration into regular operation.

3.2.8 Adapt Infrastructure and Monitoring

The complexity of the network should be checked, and the ports considered. Integration of the network can be very costly (Hybris Commerce Suite). Bottlenecks also have to be taken into account. This also involves checking the global service: In the case of local components, it is important to check whether they can also meet requirements at a global level. Further details are provided in the Monitoring.

3.2.9 Network/Bandwidth

- Where will the cloud solution be operated (consider latency time)?

- What kind of demands does the cloud solution place on the connection? Is there anything in particular that must be taken into account here?

- Does the internal Internet provider’s bandwidth have to be increased (geo-caching)?

3.2.10 Handover

To ensure smooth operation of the cloud solution, the team responsible (hotline, 1st Level, 2nd Level) must be informed and be integrated in the documentation process. Existing ITSM processes can help to flesh out the structure of the documentation. The aim here is to provide a graphical and contextual description of the new solution, together with the accompanying IT service management processes, so that the relevant teams can be quickly identified and informed if problems arise. We therefore recommend clarifying who is responsible for the handover already during the design phase.

It should be noted that monitoring layers in the various solutions work differently. IaaS solutions normally expect standardized messages for example. It is important to have a holistic view of monitoring throughout the company (see Monitoring).

3.2.11 Extensibility

One of the benefits of a cloud solution is that capacities can easily be ramped up further down the line if required. The process and the general set-up (responsibilities) should be checked here in order to prevent any nasty surprises.

How is extra capacity procured? On demand? Or must every increase be negotiated separately? Smart alignment of availability periods with operating periods (shutting down at weekends for example) makes it possible to reduce costs.

3.2.12 SAP Landscape Governance/Roadmaps

Firstly, we urge you to follow the *SAP Runtime Recommendations*:
https://wiki.scn.sap.com/wiki/display/SLGB/Landscape+Recommendations.

In addition to this, it is important to pay attention to the *roadmap* for the solution in question. A lot of money can be saved here, especially during roll-out activities. With SAP's current integration plans, synergies are highly likely.

The fundamental questions should be as follows:

- Is there a transport system between the landscapes?
- What does an ideal landscape look like? (A three-step landscape architecture or two-step?).

It is also necessary to adapt the cloud solution's release cycle (four-weekly for example) to the needs of the company. If the solution has to be validated (in the case of medical technology for example), it might not be possible to implement it.

3.2.13 Personnel: Training

Training is essential for all employees who will be involved with the new cloud solution, and should be planned as early as possible. This can help to significantly reduce the duration of the project.

The fundamental questions should be as follows:

- Who is the technical owner of the new solution?
- Who can book services from the cloud provider?
- What does the role concept look like?
- Who can release a tenant?
- Who is the system owner?
- Who is the system administrator and what authorizations does s/he have?
- Who is responsible for what?

Important: **Responsibility matrix – Who does what?**
Responsibilities must be clearly defined.

All relevant employees should be made aware of the ramifications of having a cloud solution (IaaS, SaaS). In many cloud solutions, the pricing and the billing model are related to the operating times. It might be possible to close systems down at the weekend or at certain other times when they are not needed in order to reduce costs. Given that these are not relevant factors in the on-premise world, employees should be made aware of them.

3.3 Switching Cloud Provider/Offboarding

It might be necessary to switch to a different cloud provider. This involves additional costs. The project phases (see Cloud Onboarding Team) then have to be worked through again. Synergies can exist in the financial review (requirements of cloud solutions). Migration of data to the cloud provider is often free of charge. In order to bind cloud customers for as long as possible however, there is a charge for exporting data to another provider.

When offboarding, the company should cease using the cloud solution. At this point it is necessary to agree on the retention periods to apply and on where the data should be stored in future. This can involve checking with the governance/revision team whether the data should be stored for reference purposes in the company's own archive or on the cloud provider's server.

We recommend thinking through the dependencies of offboarding/switching provider already during the implementation project so as to avoid nasty surprises or increased costs further down the line. This point should be considered already during selection and price negotiations.

4 Security

This chapter deals with the main security-related considerations to be dealt with when implementing and operating hybrid landscapes. The points discussed in the Cloud Onboarding Team chapter, such as security assessment, data ownership or Switching Cloud Provider/Offboarding will be covered in more depth here. This chapter also provides information about hidden costs that can arise in security operation and management.

The purpose of information security is to ensure adequate protection of all information in the company. Security risks are derived from risk management and should be evaluated in accordance with the likeliness of them occurring and on the potential damage that can arise. Options for dealing with these risks should be subjected to a cost and benefit analysis that examines the level of threat. By minimizing the likeliness of these situations occurring and the potential damage that can arise, the potential risk can be reduced.

Unlike in standard on-premise operation, the governance of security and compliance in a cloud computing scenario is to some extent the responsibility of the cloud provider. Prior to the implementation of a cloud service, it is therefore necessary to perform a risk analysis. This should involve examining the provider's security policies and how it handles personal data in light of the national data protection regulations, together with the compatibility of these points with the company's own compliance policies.

4.1 Security Assessment

A fundamental organizational problem arises during cloud computing due to the provisioning of cloud services initially not requiring the involvement of the IT team. In practice therefore, cloud products are often ordered directly by the LOB. Only once they are operational does it then become apparent that master and transaction data are required, together with a central user management concept.

A further problem in this regard is that security requirements in connection with the cloud service are not examined, which can result in the company’s IT being compromised and even cause legal problems to arise.

It is therefore advisable to involve the security and compliance teams and data protection experts right from the start in order to prevent the landscape being endangered by substandard integration. Ideally the security assessment should be given the highest priority of all.

At the same time it is not enough to simply perform the security assessment for the implementation of a service, as services can change during the course of their life cycle. Thought should therefore be given to arranging security assessments at regular intervals.

Both the assessment itself and the implementation of relevant measures can demand quite considerable preparation in advance. Measures arising from the security assessment can also be contractual in nature, which of course is a problem if the agreement has already been signed. Depending on its complexity, this process can take up to a year to complete and should therefore be scheduled for as early as possible. In the context of SAP Cloud Products, it is advisable in addition to the assessment of the specific cloud product to examine SAP itself as a cloud provider, along with its data centers. As many SAP security policies and processes are valid for multiple cloud products, this saves time if further SAP cloud products are implemented. Individual products can differ greatly from one another however, especially in the case of acquisitions. The scope of the assessment should therefore be defined at the beginning.

In addition to the assessment of the cloud product, it is also important for integration into the on-premise landscape to pay attention to the integration components, such as reverser proxies, firewalls or application gateways. While cloud providers often go to great lengths to protect their data centers from attacks, adequate security measures also have to be enacted by the customer. When operating hybrid environments, companies therefore need to pay special attention to protecting their own on-premise systems.

How exactly an assessment is carried out is something to be decided by the company in question. Various frameworks and recommendations are described in publications dedicated to this topic. Two common frameworks and an SAP source are described below.

4.1.1 CSA Cloud Controls Matrix

To analyze the risks arising from using cloud computing providers and to enact appropriate security measures, the Cloud Controls Matrix (CCM), part of the non-profit organization Cloud Security Alliance (CSA), offers a comprehensive framework for evaluating and analyzing security risks and the corresponding measures.

The current version of this framework encompasses a detailed collection of security principles and concepts divided into 16 areas:

1. Application & Interface Security (AIS)
2. Audit Assurance & Compliance (AAC)
3. Business Continuity Management & Operational Resilience (BCR)
4. Change Control & Configuration Management (CCC)
5. Data Security & Information Lifecycle Management (DSI)
6. Datacenter Security (DCS)
7. Encryption & Key Management (EKM)
8. Governance & Risk Management (GRM)
9. Human Resources (HRS)
10. Identity & Access Management (IAM)
11. Infrastructure & Virtualization Security (IVS)
12. Interoperability & Portability (IPY)
13. Mobile Security (MOS)
14. Security Incident Management, E-Discovery & Cloud Forensics (SEF)
15. Supply Chain Management, Transparency and Accountability (STA)
16. Threat & Vulnerability Management

This framework is part of a collection of standards for cloud computing. It contains CloudAudit, the Cloud Trust Protocol, and the Consensus Assessments Initiative Questionnaire (CAIQ). This security-based questionnaire provides cloud customers with a useful tool for analyzing and benchmarking cloud providers: https://cloudsecurityalliance.org/star/cloud-customer/.

4.1.2 ENISA Risks of Cloud Computing

A study published by the European Union Agency for Network and Information Security (ENISA) entitled "Cloud Computing Risk Assessment" contains a cloud computing risk analysis from the point of view of the cloud customer.

Policy and Organization Risks
Lock-in
Loss of governance
Compliance challenges
Loss of business reputation due to co-tenant activities
Cloud service termination or failure
Cloud provider acquisition
Supply chain failure

Technical Risks
Resource exhaustion (under or over-provisioning)
Isolation failure
Cloud provider malicious insider - abuse of high privilege role
Management interface compromise (manipulation, availability or infrastructure)
Interception data in transit
Data leakage on up/download, intra-cloud
Insecure or ineffective deletion of data
Distributed denial of service (DDOS)
Economic denial of service (EDOS)
Loss of encryption keys
Undertaking malicious probes or scans
Compromise service engine
Conflicts between customer hardening procedures and cloud environment
Legal Risks
Subpoena and e-discovery
Risk from changes of jurisdiction
Data protection risks
Licensing risks

Table 1: ENISA Risks of Cloud Computing

ENISA analyzes the likeliness of security risks occurring and the possible consequences of this, before going on to compare risks arising from cloud computing with those arising in an on-premise landscape. ENISA also classifies risks as either political, organizational, technical or legal.

The ENISA study provides valuable insights into factors to be examined when performing the security assessment of the cloud solution. It also describes best practices and security measures for reducing risks.

4.1.3 SAP Cloud Security Framework

For SAP products in particular, the SAP Cloud Security Framework provides a handy introduction to the relevant security checks and measures. The document is published by SAP on request and contains measures, policies and checks that are adopted/performed by SAP in order to meet compliance and security standards. The document covers most SAP cloud solutions, although individual cloud products are not covered. It deals with the subject areas information security, data protection and compliance in general, while also going into the specific differences that apply for each cloud service. It should be stressed that the same standards apply for both non-productive and productive systems, although only productive environments are checked by auditors.

4.2 Compliance and Data Protection

When implementing cloud products it is important to ensure that all requirements and regulations the customer has to comply with are also complied with by the cloud provider. In addition to data protection requirements, the cloud user also needs to comply with the required legal provisions.

In Germany, these include requirements arising from the Telecommunications Act (Telekommunikationsgesetz/TKG), stipulations regarding the processing of fiscal data contained in the General Fiscal Law (Abgabenordnung/AO), stipulations regarding the processing of account-related data contained in the German Commercial Code (Handelsgesetzbuch/HGB), and provisions contained in the German Criminal Code (Strafgesetzbuch/StGB).

In the case of cloud computing, it is particularly important to check compliance with legal data protection requirements, as the European General Data Protection Regulation (GDPR) stipulates that cloud users are responsible for the data security in relation to third parties. In all cases where data is processed in the cloud, the cloud user is responsible for this data and has to ensure that the data on the cloud provider’s servers is handled in accordance with the prevailing legislation.

An order processing agreement also has to be drawn up with the cloud service provider. In addition to the general conditions of the GDPR, the following points demand close attention. This includes listing all subcontractors used. The cloud customer must be accorded a right of objection so that s/he has the option of withdrawing from the agreement If any additional subcontractors are used.

A further point is the assertion of rights of control. As this is not possible in situ, the right of control can be rendered by means of certificates. It is necessary however to check whether the specific cloud service is covered by the scope of the certificate. This can often only be guaranteed by examining the auditing logs.

It is also necessary to guarantee the option to change provider, to export data, to delete data subsequently and for the data to remain the property of the company.

4.3 Compliance and Certification Audits

An established instrument for checking that compliance and security standards are observed is to involve independent auditors. From the customer’s point of view, certification renders the cloud provider more trustworthy. As the various SAP solutions are operated in different data centers and under different technical prerequisites, it is essential to check various standards depending on the area of application, geographical restrictions and regional jurisdiction. As far as SAP is concerned, the various cloud solutions are certified in accordance with the following standards:

- ISAE3402/SSAE18-SOC 1 Type II and/or SOC 2 Type II
- ISO 27001:2013
- ISO 22301:2012
- ISO 9001:2008
- BS 10012:2009
- PCI-DSS 3.2

The corresponding certificates can be viewed in the SAP Cloud Trust Center for the corresponding solutions. It is important however to check whether each certification is valid for the cloud solution being employed.

It is also advisable to request the test reports under Non-Disclosure Agreement (NDA) and to examine them in accordance with the customer's internal security policies.

4.4 Security Measures

Following on from the security assessment of the solutions to be implemented, various security measures can be adopted in order to minimize the risk of them occurring and the potential damage that can arise. The following is a selection of some of the measures and best practices that can be adopted.

4.4.1 Penetration Testing

As hybrid landscapes involve the integration of cloud systems with on-premise systems, it is especially important for the central integration components to be secured. The test reports for each cloud solution certify the performance of regular penetration tests. The customer's infrastructure should be tested and strengthened accordingly however. It might therefore make sense for the cloud solution to be subjected to penetration tests on the customer side. The performance of these tests should be agreed with the provider however, and to examine the agreements, as penetration tests can also impact other customers, especially in public cloud environments.

4.4.2 Encryption and Interface Authentication

Communication in cloud and on-premise systems should always be encrypted. This involves employing secure encryption protocols and technologies, and regularly ensuring that the latest version is being used. Non-secure cryptographic algorithms and cipher suites should not be used.

For the authentication of interfaces, certificates or secure procedures such as OAuth2.0 should be used. If possible, the use of basic authentication comprising user and password should be avoided. While regularly updating certificates does serve to heighten security, the amount of time and effort that this involves in larger distributed environments should not be underestimated.

In addition to encryption of the exchange of data (data-in-transfer security) via the corresponding interfaces, it is also important to ensure encryption of the data in the cloud (data-at-rest security) and to store the corresponding codes securely. This applies to the corresponding tenants, containers or data backups. The security assessment should include a careful examination of these security questions and the adoption of corresponding measures. Ideally there should be mechanisms in place to allow the customer to define the codes him/herself. This helps to reduce the risk of unauthorized access by the provider.

4.4.3 Hardening and Patch Management

When implementing cloud services it is important to not rely entirely on the adoption of security measures by the provider, as the company's own infrastructure also requires hardening and maintenance as soon as the systems are integrated with one another. In order to close potential security breaches, it is particularly important to carry out regular maintenance of the on-premise integration components in the SAP cloud environment. Critical weaknesses regularly arise in connection with the Cloud Connector for example. Resolving these security breaches should therefore be an integral part of Change Management in order to enable rapid action where required.

Depending on the operating model (IaaS, PaaS, SaaS), the infrastructure, platform or application is operated and maintained by the provider. Also depending on the operating model, this means that different components have to be patched by the customer. It is therefore necessary to clarify who is responsible for third-party libraries and how to test most efficiently. Does the operator offer tools to check for weaknesses in customer developments for example?

As new infrastructure components, such as web application firewalls, reverse proxies or Cloud Connector are set up when designing hybrid landscapes, the costs for the maintenance and further development of these components increase commensurately.

4.4.4 Identity Management (IDM)

Unauthorized access to company data can cause serious damage to companies and customers. Compared to on-premise applications, which are often only accessible from the corporate network, cloud services can be accessed via the Internet, which hugely increases the risk of unauthorized access. As cloud and on-premise systems are often closely integrated with one another, the danger in such cases is that on-premise data will be compromised too.

To reduce the risk of misuse of data, a central cross-system Identity Management System (IDM) should be set up in hybrid landscapes with different systems and corresponding authorization concepts. It is necessary for example to ensure that users are locked when they cease working for the company, as cloud services can also be accessed from outside the corporate network.

Corresponding processes, such as creating or locking users, and assigning authorizations, are checked during audits and revisions in accordance with standards such as ISO 27000, SOX, BSI, or the EU GDPR.

Starting from a certain size of company, equating to a medium-sized company for our purposes, the effort required for manual user administration and authorizations should not be underestimated, and can only be dealt with efficiently by means of automation.

Many companies therefore already employ IDM systems while still working solely with on-premise systems. In the context of hybrid landscapes, this makes it necessary to check how users and authorizations can be managed in cloud systems.

A standard for cross-system user management is the System for Cross-Domain Identity Management (SCIM). This provides a simple set of commands for creating, updating, reading and deleting, and is based on the interface technology REST and data format JSON. Many SAP cloud products already support SCIM by default.

In addition to the direct connection of the cloud services to the IDM system, the use of the SAP Cloud Platform Identity Provisioning service should also be checked. This provides standard integration with most SAP Cloud Platform services. Mapping of user attributes therefore ideally only needs to be done in one place, namely between the on-premise IDM and SAP Cloud Platform Identity Provisioning. SAP Cloud Platform Identity Provisioning is particularly relevant in cases where the company does not operate its own IDM for its own user management.

With regard to EU GDPR, it is necessary to check whether the respective cloud application supports mechanisms to delete user information when required.

4.4.5 Access Management (IAM)

In addition to maintaining users and authorizations using a central IDM system, it is also advisable to consider using a central identity provider for authentication.

A very common standard for the exchange of authentication and authorization data in the Internet is Security Assertion Markup Language 2.0 (SAML 2.0).

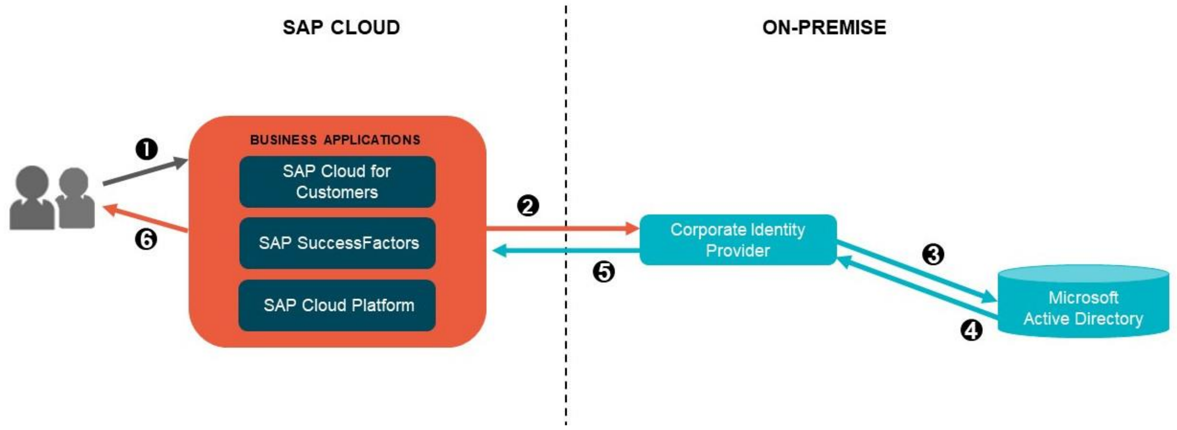

Figure 2: SAML Authentication

Figure 2 illustrates a simplified process where authentication is delegated to the corporate identity provider. In this example, the corporate identity provider checks whether a valid active directory user exists and then returns an access token so that the user can authenticate him/herself. This type of system has a number of advantages.

Single sign-on can be used across cloud and on-premise systems for example. After logging on, the user does not have to enter access data again when calling the corresponding cloud application, as authentication takes place in the background via the identity provider (IDP).

It is also possible to define various security policies on the corporate identity provider. These can be used for example to stipulate that a user logging on from outside the corporate network has to use two factor authentication.

If the company does not run its own identity provider, it can use SAP Cloud Platform Identity Authentication Service (IAS) instead. Most cloud services offer standard integration. It might therefore make sense to switch IAS before the corporate identity provider in order to speed up the connection of SAP Cloud Platform services.

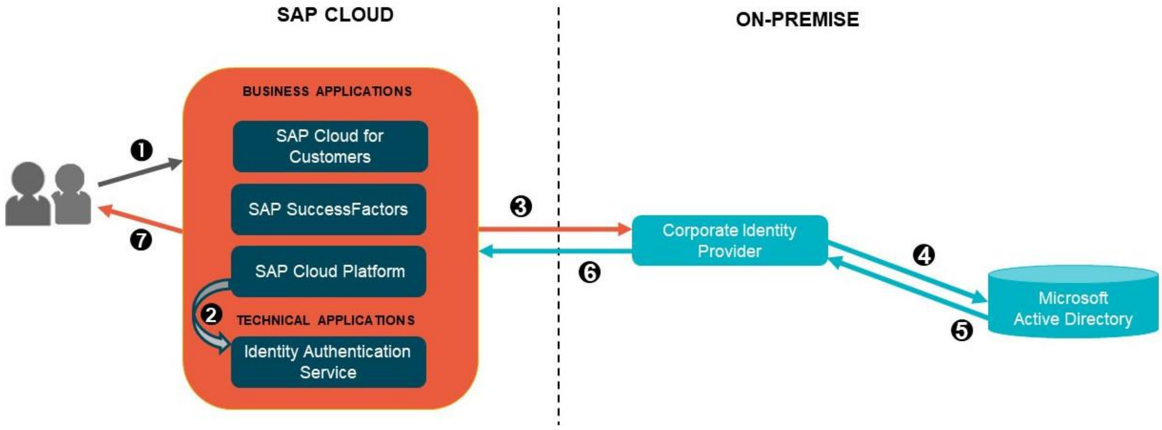

Figure 3: SAML Authentication via IAS

Figure 3 illustrates authentication via IAS and the corporate identity provider. In addition to standard integration with most SAP cloud services, further advantages with this type of system are functions such as the connection of different user stores for external users and users for SAP Support, who do not have to be maintained together with internal users in the active directory or should be kept apart in accordance with the security policies.

From the point of view of risk, it should be noted that a central identity provider is a highly critical component in the system landscape. If this component is unavailable for whatever reason, no users can authenticate themselves. In order to avoid this eventuality, effective high-availability measures should be adopted.

In order to prevent performance bottlenecks during login, globally operating companies should implement a decentralized setup (over multiple regions).

This can result in unplanned costs if the central IDP is unavailable or if there is no decentralized setup. Maintaining authentication policies and general operation should not be underestimated either.

Depending on the license model, significant costs can arise, for example if the provider charges by login request, and the number of connected systems continually increases.

With regard to mobile applications for iOS or Android, the cloud services should ideally support OAuth. With pure SAML authentication, the session is often lost if the user closes the app or the operating system suspends the application. In practice, users therefore have to authenticate themselves several times a day. Using OAuth it is possible to keep the session alive if the app is closed and restarted. The initial authentication here works via SAML 2.0 Bearer Assertion Flow for OAuth. Once the user has authenticated using SAML, the OAuth token is issued. The duration of the token's validity depends on how it has been configured.

4.4.6 Landscape Architecture and Network Security

The various SAP cloud solutions have different technological foundations. In the case of direct integration with third-party systems, all interfaces should be listed. They should also be checked in order to determine whether they can be called directly or whether middleware is required. In a hybrid landscape, it is important to carefully check whether dedicated components such as the Cloud Connector are required if using SAP Cloud Platform, or whether the connection is established using other customer-specific reverse proxies and firewalls that are supported by the provider. Ideally, the connection to the SAP Cloud Platform should take place via a central component so as to increase maintainability and to avoid backdoors.

Unfortunately however, mature hybrid landscapes often do not possess a unified architecture. In practice this leads to hidden costs for maintenance, troubleshooting, or closing security breaches.

4.4.7 Mobile Device Management (MDM)

Many cloud solutions offer mobile applications. With regard to mobile device management, it is necessary to check that the cloud solution can be accessed from devices that are not managed by the corresponding MDM solution. This can be done by rolling out client certificates for example, or using key value authority process. It is also necessary to check whether it is possible to comply with the company’s security policies during mobile access or for example if access can happen without authentication.

4.4.8 Backup & Recovery

Depending on the operating model (and especially so in the case of PaaS and SaaS), the operative tasks, such as regularly backing up data, are passed on to the provider in cloud computing scenarios. The customer therefore no longer has direct control over the execution and storage of database backups. This makes it more important still for these tasks to be performed conscientiously, so that the systems can be restored should this be necessary.

The ISO 27001and SOC-2 certifications also include checking the processes for execution and storage of data backups. An example of this is checking how often backups are created and how often they are replicated in backup data centers so as to minimize the risk of loss of data if the data center suffers an outage. A maximum period that loss of data can occur for is defined in the SLAs in accordance with the backup process.

A risk arises in hybrid landscapes on account of the integration of on-premise systems. Due to the master data and transaction data being replicated with the on-premise systems, inconsistency between systems could arise in case of loss of data on the cloud application side. In cases like this there is the option of restoring the on-premise systems to the same state as the cloud application. In practice this is often not done though, as it would involve resetting the ERP system for example. Another option is transferring all changes again. In the case of loss of data, all messages therefore have to be transferred to the system again.

In a hybrid landscape with various SLAs, elaborating this type of disaster recovery concept (DSR) demands a huge amount of effort. Cloud providers ensure that corresponding DSR tests are carried out. These tests are only performed dedicatedly for systems that the company is responsible for however, and which do not involve the customer. This means that concepts developed by the customer cannot be checked sufficiently.

If possible, this type of DSR test should be performed before implementation and at regular intervals, with the involvement of all integrated systems. All of which can result in increased effort during operation.

5 Integration

Although the service provider is often responsible for operating the cloud services (depending on the SLA in question) in the context of hybrid system landscapes, the customer is always responsible for ensuring smart integration (“ownership”).

The following sections deal with system integration, especially with regard to process integration and data integration. In the context of increasingly complex hybrid landscapes, business processes (still) run across multiple systems. „Digitalization is increasing the complexity of system landscapes. Business processes do not halt at the boundary between one application and another. Instead, they are made up of or orchestrated by multiple applications.“[3] Smart system integration can therefore even offer an opportunity to improve processes, especially in terms of quality and speed.

System integration can therefore provide an opportunity to improve processes, especially in terms of quality and speed. This means that system integration is one of the drivers for automization - especially in light of Industry 4.0.

5.1 At what point does system integration become relevant?

System integration is essential in hybrid scenarios and therefore should be given thought to right from the very start. When selecting which services to implement at the very latest, it is necessary to check the extent to which integration into existing scenarios is necessary. By the time systems or cloud services go live it might already be too late.

[3] Steffen Pietsch at the DSAG Technology Days event, 2019.

5.2 What needs to be taken into account when integrating systems into hybrid landscapes?

In the context of system integration[4], numerous things should be taken into consideration, ideally already when selecting the systems and services to be implemented.

The first question to examine is whether the cloud solutions or on-premise solutions can actually provide the required level of integration. This has a direct effect on the amount of effort that will be involved during the implementation project and subsequent operation, with regard to integration into monitoring for example. It is essential to have interfaces that use modern message formats and transport protocols in order to support the required process. It should be ensured that the technologies used for the interfaces are compatible with the company's integration strategy and that the required tools are available. If there is a need for additional tools, the effort involved can be taken into account at an early stage, which might actually result in other services being preferred.

It is also advisable to check whether (additional) on-premise systems are required for integration with the existing IT landscape. Reverse proxies might be required for example that still have to be installed on-premise and integrated with the corresponding network segments (DMZ for example). If the on-premise systems are hosted in a (private) cloud, partners can be involved at an early stage, and the additional effort involved can be taken into account.

The existence of pre-configured integration processes (“Integration Content”) can constitute a major advantage. Due however to the different deployment models of the cloud solutions (SaaS as opposed to PaaS) and the wide range of options for building and using integrations, this has to be examined and estimated on a case-by-case basis. It is not possible to make a general recommendation here, since system integrations are simply too individual to allow this. A general recommendation however is to carefully check the delivered content so that is possible to estimate the extent to which it can be used for the planned scenario. It could be that the content does not meet the requirements and therefore has to be enhanced. The effort involved for this is also something that should be identified at an early stage. A distinction is made here between purely configurable content that does not allow major adjustments, and content that allows unlimited copying and modification. In the latter case however, it

[4] The SAP Integration Solution Advisory Methodology can help with system integration: https://blogs.sap.com/2020/05/14/new-version-of-the-sap-integration-solution-advisory-methodology-template-released/

should be noted that individual modifications to the content might make it impossible to run automatic updates to new versions.[5]

Many software providers, including SAP, pursue an “API first” strategy. This involves providing interface modules, mostly in the form of OData services or Web services, in order to connect the system. It is therefore advisable to carefully examine the software provider’s API repositories (SAP Business Hub for example) before deciding whether to use these technologies. If extensive use is made of APIs, consideration should be given to using a corresponding management tool, such as SAP API Management. These tools make it possible to meet the requirements in terms of API provision, security, traffic management, metering, and analytics.

Encryption, authentication, and authorization should meet the requirements set by the company and be compatible with its integration strategy. As various different procedures can be adopted, it is only possible to make a general recommendation. The requirements of the services to be integrated also have to be taken into account, in particular the question of whether these requirements are fulfilled by the certificates currently in use.

Special attention should also be paid to the data models. It is important to find out whether the data models of the systems to be connected match each other semantically, in other words whether data consistency can be ensured. Timely collaboration with the line of business is therefore recommended, so that any additional effort can be estimated and planned for.

It is also necessary to check whether the SLAs for integrating a service are compatible with the SLAs in your company. If a critical business process has a required availability of 99.9% for example, but interface availability of only 95% is ensured, a solution must be found.

In the case of cloud solutions, especially SaaS, the company’s IT does not always have the same level of insight into the integration layer as in familiar on-premise systems. Unintentional mass replications should be prevented however.

It is also important of course to check whether the networks can cope with the additional load arising from the planned integration scenarios. Depending on the importance of the business processes in question, it might be possible to implement additional requirements and to reduce the risk of outages arising from redundancy, and to improve the data transfer speed improved (latency and bandwidth).

[5] With regard to the Prepackaged Integration Content for SAP Cloud Platform Integration, there is now a solution available for this purpose: „Integration Flow Extension“ https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/d3741720e29842e4bf547dcd66139f7f.html

5.3 What costs can arise?

Integration costs are highly variable. It is not possible to provide specific figures here. Our purpose is more to detail cost-generating factors and thus to raise awareness of hidden or unexpected costs that can arise. A general observation is that there is a tendency to slightly underestimate the effort and cost involved in system integration. In this regard it is particularly important to achieve transparency and to check and estimate the costs at an early stage, ideally before selecting the systems and services to be implemented.

Licenses: Are the components and services required for the planned integration already included, or will additional licenses or fees be necessary? Are these one-off costs? Or recurring costs that are perhaps based on a quantity structure?

Implementation: What level of effort is required for implementation? To what extent do the interfaces or the delivered content require modification? How easy is it to connect a service? Can all efforts be managed internally? Or is external support required from a partner or from the service provider itself?

Middleware: Is the required middleware (SAP Process Orchestration or SAP Cloud Platform Integration for example) already available? Are the middleware licenses sufficient? Are the middleware's system resources sufficient, or do they need to be enhanced?

Certificates: Are all required (public signed) certificates already available? How often do these need to be renewed? What are the costs arising from this?

Indirect Use: Does the planned system integration count as "indirect use"? It is advisable to discuss this matter with a member of the SAP sales team.

Infrastructure Components: Which costs have to be calculated for additional components, such as reverse proxies or gateways?

Networks: Do network components have to be enhanced in order to achieve better latency and bandwidth? Does this necessitate changing the agreements with the Internet providers? Are additional redundancies needed in order to keep the required SLAs?

Coordination: Does this integration project involve distributed teams that have to collaborate with one another?

Operation: What level of effort is required for monitoring? Which regular activities have to be performed with regard to interfaces? How complex is the handover?

Skills: Are the company's employees already acquainted with the technologies being used? What kind of extra know-how needs to be acquired? What kind of know-how needs to be purchased from external resources?

5.4 Additional Notes

For more in-depth information on the subject of integration, the following are recommended:

- CIO Guide: Process and Data Integration in Hybrid Landscapes
- YouTube video of Steffen Pietsch's keynote presentation at the DSAG Technology Days 2019 (in German)

6 Operation

Integration of SAP Cloud solutions with the existing SAP on-premise landscape requires effort in SAP Basis and in other groups involved in operation, both for the initial go-live and for subsequent continued operation.

Depending on the size of the IT organization, consideration should be given to creating virtual teams for cloud solutions. Cloud solutions are not only implemented in the SAP environment.

With the introduction of cloud solutions, the existing landscape is enhanced once more. Often cloud solutions are built without a corresponding scale-down of the old solutions. The growth that arises with the introduction of cloud solutions must therefore be taken into account in all aspects of operation.

Growth is not just a question of mass. It also translates into an increase in information about new software and technologies. As a landscape becomes more complex, the effort involved in coordinating with internal and external partners and providers grows too. When errors occur, the analysis effort grows considerably, and responsibilities shift.

The help desk personnel (1st level) have to deal with new concepts and systems. In "Operating/Application Support" (2nd level), where tasks such as central monitoring, job control and routine tasks are performed, an understanding for the new situation must be acquired. The teams for the individual applications or the infrastructure (3rd level) need to master the new technologies, and it must be clear how a connection functions at all levels.

6.1 Organizational Prerequisites

6.1.1 Procurement Process/Onboarding

As described above under Discovery & Cloud Onboarding/Offboarding, we recommend involving the IT team already during the procurement process for cloud services and purchasing, as only the IT team can have a complete overview of all integration aspects. The security/compliance team should also be involved. It is necessary here to check whether the cloud solution conforms with the company's security standards.

6.1.2 Incident Management

Depending on the solution/applications, users (external customers and employees) must be enabled to create messages to report incidents. Editing SAP messages (OSS messages/SAP Support Portal) must remain in the Basis, although thought must be given to how the various solutions for handling incidents can be connected.

For more information, see Incident Management.

6.1.3 Problem Management

The same rules apply here as for familiar on-premise solutions. As with incident management, external service providers must also be involved.

Not every service provider and provider is able or willing to work in the individual customer’s “software/solution for problem management”.

6.1.4 Change Management

The resolution of change dependencies becomes far more complex. This also depends on the scope and frequency of changes in the various cloud solutions. We therefore recommend creating a cross-solution change and release calendar.

It is necessary to clarify how changes can be integrated with the structures and processes without additional downtimes occurring in the applications. Existing definitions for downtime and SLAs might need to be modified.

- System copies over all application chains
- Downtimes of cloud solutions
- Who is informed when downtimes or incidents occur?

For more information, see chapter 7 Hybrid Lifecycle Management under 7.2 Incident Management and the information about SLAs under 3.2 Service Level Agreements.

6.2 Differences Between Individual Cloud Concepts

IaaS, PaaS, SaaS. These different approaches all have their own particular advantages and disadvantages, and need to be appraised in accordance with the specific requirements. The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) provides a description of the differences between the various concepts in Cloud Computing Basics.

An overview of these processes can be found under Public Cloud Operations in the SAP Expert Portal. Without going into too much detail regarding the differences between these three categories, it is important to consider the implications for the company’s IT setup if one or the other of them is introduced. What is the company looking to achieve?

There are a large number of questions to be dealt with here. How do I deal with licenses if I opt for IaaS and therefore do not need an on-premise infrastructure and therefore simply order infrastructure from a hyperscaler? Can I also install software acquired as part of an enterprise license on servers that are not on my company's premises? With IaaS, there is no need to think about servers and other forms of "physical" infrastructure, but all other questions need to dealt with consistently, such as data backups and monitoring. Taking SAP Basis as an example, there are virtually no changes at all if the IaaS approach is adopted.

In the case of PaaS, the question of the operating system license is possibly answered right from the start, as the license is a central part of the provider's service. Regular computer backups are also created. Somebody still has to install the software however, and has to deal with issues by means of support agreements or by calling on external expertise. Obscure (small) bundles are ideal candidates to be moved into the cloud. Taking SAP Basis as an example once more, database administration could be moved into the cloud, as this is made available by PaaS service providers.

If database administration is to be moved into the cloud as well, SaaS is the option of choice. The solution is available at the touch of a button and just needs to be filled with data. Integrations of these solutions are still necessary and also generate a certain amount of effort in SAP Basis.

Whichever of these three variants is adopted, it is necessary to check that the SLAs are adhered to. Only by consistently examining these SLAs can possible benefits such as cost reduction be ensured. Processes like incident management or problem management are still required for "operation" however. In other words: Not all (IT) tasks can be outsourced by adopting cloud solutions.

6.3 Landscape Management – Process in SAP Solution Manager

The purpose of the Landscape Management process is to collect data from the IT landscape via the *System Landscape Directory* (SLD) and *Landscape Management Database* and to make this data available.

This data can be made available in order to calculate changes in the landscape, such as updates, upgrades and conversions. It can also be made available to other functions, a particular example being IT landscape monitoring. The introduction of cloud solutions has made it possible to operate a hybrid landscape comprising both cloud and on-premise systems. As far as possible, the SAP-related cloud systems should be integrated in Solution Manager. This is necessary for continuous monitoring of the SAP landscape.

The Landscape Management Process page on the SAP Support Portal describes this core function and provides background information regarding the various deployment models and the big picture of Change Management, implemented with either the

Maintenance Planner – for a system managed by the customer – or by subscribing to cloud services.

This information is accompanied by an overview of

- Integration of the Landscape,
- Development,
- Transport Tools
- and enhanced options for operation with SAP LaMa.

6.4 Application Operation

Certain tasks and activities that have to be performed are also required for the operation of cloud solutions. Some of these are listed below. Some of these activities have to be performed by the company's own SAP Basis team.

The following points are intended as a *checklist* for operations that should be performed. In each case it is necessary to check who is responsible. In a public cloud, the cloud provider is responsible for many of them. In a private cloud, this depends on the Service Level Agreement (SLA).

Checklist

- ✓ Start/Stop, Maintenance
- ✓ System Copy, System Refresh
- ✓ Monitoring
- ✓ Certificate Management
- ✓ Job Control
- ✓ Testing
- ✓ Coordination of system downtimes/system updates/ system patches and so on. The effort involved can be considerable and should not be underestimated.
- ✓ Who creates the documentation (operating manuals) for the cloud solution - also in conjunction with the existing on-premise solutions?
- ✓ Credit Request/Penalty: If the SLAs are not fulfilled, do they have to be billed for?
- ✓ When does the cloud solution go live?
- ✓ What prerequisites apply for the go-live?
- ✓ Alignment with the involved groups
- ✓ Publication of an operating manual
- ✓ Who is responsible for what?
- ✓ Who can create OSS messages?
- ✓ How enhanceable/scalable is the cloud solution?
- ✓ How to deal with “validated systems”?

6.4.1 Synchronize Downtimes

How can it be ensured that this information can still be used, for example in system monitoring of the Solution Manager, during planned work?

Planned work in the cloud solutions must be announced on the operating side so that this information can be brought together with the on-premise solutions. Possible influences for downtimes must be taken account of and it must be assumed that an interface will not be available on the on-premise side during the downtime. During this time there should not be any reporting of problems arising with this interface for example. Efforts should also be made to ensure proper coordination of work between cloud and on-premise systems.

6.4.2 Portals for Cloud Solutions

The large number of portals represents a significant challenge. When starting a cloud project, the following questions need to be examined:

- Which URLs are available?
- Which user group and/or roles are intended for which portal?
- Which products can be found in which portals?
- What task does the portal have?
- Who manages the authorizations?
- Which components should be relevant for creating support calls?

6.5 Reporting

The SLAs of the various solutions need to be monitored in order to ensure stability and availability, and to be enforce claims against the provider if necessary. By logging on to a website with just a few clicks (in SAP Solution Manager with User Experience Monitoring – UXMon) it is thus possible to check whether the system is available. This monitor can then be used independently of the defined threshold values to trigger an alert or to determine the availability of the solution.

It is important for customers to monitor the SLAs. It is then possible to generate reports on these SLAs on a monthly basis and to make these available to the people responsible. It is also imperative to check reports published by providers.

6.6 Monitoring

For stable operation of an SAP landscape, monitoring of all connected systems and components is desirable. This should include facets such as system monitoring (CPU, hard disks and so on) and interface monitoring through to simulation of individual click sequences made by users and complete business processes. Reports dealing with the chronological evolution of KPIs also facilitate proactive behavior and thus help to significantly reduce the potential for incidents to arise.

An alignment of changes/transports,and most particularly of downtimes, is required in order to prevent false alarms.

Some cloud solutions provide standalone or open source-based monitoring solutions via different UIs. Customers cannot make full use of these and/or have limited authorizations when using them.

In a hybrid landscape it is therefore essential for customers to ensure monitoring of their own landscape, including all cloud applications, and preferably to have this integrated with existing monitoring solutions.

6.6.1 Central Monitoring Cockpit

Ideally there is a central monitoring user interface where it is possible to recognize immediately where errors are occurring. There should also be views that provide information about the various systems depending on the role (admin, helpdesk, operation and so on) and the applications (sales, service, logistics and so on). This information must be merged from various monitoring solutions across technological boundaries.

SAP Support Launchpad offers a central Monitoring Cockpit, where the SAP Cloud Services can be successively integrated:

Cloud Availability Center: https://launchpad.support.sap.com/#/cacv2

6.6.2 Technical Monitoring

At some point it is inevitable that an incident will occur in every cloud solution, whether it works as a function module in the background or for example as part of the B2C shop. Regardless of the cause, this incident will be reported via technical monitoring (or by a user). It is essential to ensure that these messages are correctly assigned. The aim must be to give the message a priority, to find the right person to deal with it, and to optimize the processing time. It might be necessary to trigger escalation.

The content of technical messages must be uniquely identifiable. In the SAP environment, the system ID or client provide a good way of classifying a message. This is more difficult in the case of messages reported by the user if s/he is on a website. Where exactly is the user, and how can the application be identified clearly here? This question also arises in the case of on-premise applications of course, although for cloud solutions identification by the “hotline” must also be possible. Whether the call (or mail) is made/sent by an external customer/user or by an internal colleague is completely irrelevant.

The requirements that apply for the on-premise monitoring solution generally also apply for the cloud solutions. It is necessary however to clarify which monitoring has to be performed internally, as operation is sometimes performed externally in the case of cloud solutions. In this respect, IaaS generally results in greater effort than SaaS or PaaS.

Exception Management must be taken care of by the provider, regardless of whether the solution is IaaS, SaaS or PaaS. System monitoring such as CPU or memory usage and disk IO can also be a good indicator. This is especially the case if metrics such as reply times increase.

Monitoring should be performed in any case for cloud solutions by functions such as E2EMon/UXMon (User Experience Monitoring). Depending on the different functions of a business process, it is also possible in the case of synchronous solutions to check access to on-premise solutions.

Login to the system should be tested at the very least. For the SLA analysis, it must be ensured when errors occur that the accessibility of the solution via the Internet connection for the agent is not the cause of the error. Depending on the relevant interfaces, these can be checked at the on-premise end at least (see Solution Manager – Interface Channel Monitoring).

End-To-End Business Process Monitoring (E2E-BPM) should take place across the hybrid landscape, as business processes do not normally only run in the cloud. The aim here must be for an application owner to be informed whenever one of these processes malfunctions.

Requirement from SAP:
SAP should provide immediate delivery of UXMon scripts for standard solutions.

6.6.3 Manual Monitoring

During manual monitoring, transactions are checked at various intervals (such as daily, weekly or monthly). This is often outsourced, which means quality cannot be ensured. We therefore recommend only employing manual monitoring during transitional phases.

6.6.4 Alerting and Incident Management

For specific events, alerts should be forwarded to the relevant incident management solution. It should be noted that alerts that are closed in the cloud solution (whether automatically or manually) also have to be closed in the on-premise monitoring solution. SAP CP Alert Notification enables the forwarding of availability alerts to SAP Solution Manager/FRUN.

6.6.5 Costs for Monitoring

The costs arising from monitoring depend on the scenario and are thus difficult to calculate. This is also due to the fact that every company has its own way of “monitoring”. In all cases it is necessary to check exactly to what extent these tasks are to be performed either manually or automatically. The costs of managing and maintaining automatic monitoring also depend on the size of the cloud solution and should not be underestimated.

6.7 Automation of Recurring Operating Tasks

In order to keep down the costs incurred for recurring tasks related to operation, consideration should be given to automating these tasks. For SAP Cloud Platform, the SAP Cloud Platform Automation Pilot provides catalogs of automated commands relating to typical tasks for the operating of applications on SAP Cloud Platform, either to restart applications or cloud databases in the event of problems, or to perform monitoring tasks with direct integration with other tools (such as an automated triggering of commands based on events sent by SAP Cloud Platform Alert Notification). Certain commands for this can be created and shared without any development effort.

6.8 Costs/Effort

We recommend carefully investigating the anticipated costs for operating hybrid landscapes. The following questions should be examined:

- What extra costs will be incurred on a one-off basis and/or on a regular basis during operation?
- Has the effort required in each group been clarified? Is there sufficient staff and capacity available?
- How can unplanned effort arising from incidents be quantified and covered for?

The most important aspects are summarized in the *checklist* on the following page.

Checklist

- ✓ The infrastructure must be made cloud-ready before cloud projects commence.
- ✓ Paradigm shift for interfaces. In on-premise landscapes, deep integration between systems using sophisticated technologies is the norm. In the cloud universe, SAP speaks of loose interconnection between systems.
- ✓ Comprehensive change and release calendars have to be maintained.
- ✓ How are the various incident solutions connected with one another?
- ✓ Is there an alignment in the SLAs between cloud and on-premise? Are these monitored?
- ✓ What URLs are available for administration of the cloud solutions? Has SAP progressed far enough with the “Trust Center” so that harmonization has been achieved, and the same channels are always used?
- ✓ Where will additional one-off/regular effort arise within the company? How is this scheduled?
- ✓ For hybrid landscapes, it is especially important to monitor the landscape in a holistic fashion and ideally to integrate this with the existing monitoring solution.
- ✓ Manual monitoring should be employed during solely during the transitional phase.

7 Hybrid Lifecycle Management

7.1 Organizational Implications

For the support organization, a hybrid landscape represents a major challenge. The following points need to be clarified:

2. Within the company, the responsibilities for cloud support and change management responsibility for the various cloud applications have to be clarified.
3. The required resources must be made available. It might be necessary for example to have a separate (virtual) cloud team for SAP Basis.
4. Training must be provided for the company's employees.

A description of the process steps and the roles involved is provided by SAP under Landscape Management Process.

7.2 Change and Release Management

7.2.1 General Comments

In Change and Release Management, we make a distinction both in the on-premise world and in the cloud environment between application changes and maintenance and infrastructure changes.

In the SAP environment, many customers make use of SAP tools such as SAP Solution Manager or the Transport Management System (TMS), but mainly still have a comprehensive ITSM tool, where all IT changes are recorded and are coordinated. In a hybrid landscape however, there is often no overview of the coordination of changes on-premise and in the cloud.

7.2.2 Release Management versus Agility

In on-premise landscapes, release cycles are frequently defined in such a way that custom features are released together in bundles. Costs are thus reduced thanks to defined testing periods, and the stability of the landscape is maintained. In the cloud, agile development is the norm, and new or changed features go live very soon after completion. The challenge in hybrid landscapes is therefore to classify all developments and to ensure a stable landscape despite having different development cycles.

7.2.3 Change Management in Hybrid Landscapes for Custom Developments

- **Cloud – Cloud:** For use in the cloud, SAP has developed the CALM tool (SAP Cloud ALM). Application management functions for the cloud are successively mapped in CALM in the same way that Solution Manager functions are for on-premise systems. This also includes Change and Release Management.

- In SAP Cloud Platform, the SAP Cloud Platform Transport Management Service can be used. This makes it possible to transport development and application artifacts from SAP Cloud Platform (SAP Cloud Platform Integration content for example). If cloud applications are developed in a continuous integration pipeline, handover from the development landscape to the delivery landscape can be defined by triggering corresponding transports from the pipeline. This allows a combination of agile development methods based on automated pipelines (for the validation of individual development changes) with clearly-defined delivery processes (for the validation of release candidates, usually with manual confirmation and controlled delivery to the productive landscape). SAP offers scenarios, interfaces and pipeline steps for this, thus facilitating the integration of a defined handover to existing pipelines.
- **On-Premise – Cloud**:

  If SAP Solution Manager and the enhanced Change and Transport System (CTS+), which offers direct triggering of transports from the SAP Cloud Platform Web for example, are already in use, this can be retained for hybrid landscapes. CTS+ allows the transport of cloud artifacts in the form of multi-target application archives (MTA) - extension of this to other cloud artifacts (that use a different format than MTA archives) is not planned for CTS+.
- The enhanced Change and Transport System (CTS+) and the SAP Cloud Platform Transport Management Service can also be used in parallel for various cloud artifacts. While this increases the complexity of the change management landscape, it also allows a smoother and gradual transition from CTS+ to Cloud Transport Management for the cloud artifacts.

- For synchronized transport of hybrid changes, integration into Change Management approaches with Quality Gate Management and Change Request Management (ChaRM) is possible. SAP offers “close coupling” with CTS+ and SAP Cloud Platform Transport Management for this purpose. This makes it possible to transport on-premise and cloud applications in bundles without any manual effort.

7.2.4 Change Management in the Cloud IT Landscape

- **Cloud – Cloud:** Customers who have spread their applications over multiple cloud providers need to acquire an overview of the planned changes and enter these in a comprehensive plan. By doing this they are aware of upcoming maintenance windows and are able to plan their own changes accordingly. Integration for this is not available. For the SAP Cloud applications, details are provided in the Cloud Availability Center.

- **On-Premise – Cloud**: An overview of all changes in the hybrid landscape is currently not available. The more spread the cloud applications are, the more complex the planning process is for changes. Whereas it was still possible to plan changes independently in the on-premise environment – which in itself was a challenge in the case of large landscapes – hybrid landscapes make it necessary to take account of predefined maintenance windows. In order to handle the ever-increasing complexity of the change process, it is important to have a clear overview of all planned maintenance activities. It is therefore necessary to access the relevant information using APIs or to provide integration in a tool, for example in Solution Manager or Cloud ALM.

Change Management Requirements Faced by SAP

- A central IT calendar in the Launchpad (for on-premise products and cloud products) and interface to other ISTM tools
- Harmonization of the downtime windows
- Zero downtime for all cloud products

Hidden Costs

- Effort arising in connection with the coordination of on-premise – cloud changes
- Additional work following on from patches in the cloud at short notice

7.3 Incident Management

7.3.1 Tools

The existing landscape determines the procedure when implementing incident management for hybrid landscapes. It is important to have an inventory of existing processes as the basis for deciding on an incident management procedure in the hybrid landscape. If SAP Solution Manager is used as the incident management tool for example, we recommend using this for the hybrid landscape.

- SAP Solution Manager
  SAP Solution Manager provides the features of an ITSM tool for on-premise applications and is perfectly equipped with the SAP Backend Feedback function for SAP.
- SAP Cloud ALM
  Cloud Application Lifecycle Management will incorporate more and more functions in the cloud that now SAP Solution Manager offers on-premise. Customers should keep up to date on the status of development. They can thus find out which features are available and find the right time to transition.

7.3.2 Integration

If an ITSM tool is already in use, it makes sense to continue using it. If an integrative solution is not available at the start, you should take appropriate organizational precautions. Incidents can also be created manually in all tools. To do this, we recommend creating the corresponding forms/queries for the cloud applications in order to request the relevant information from users (the URL of the application where the problem occurs for example).

At the same time it is essential to involve the service desk and to draw up a list of the existing cloud infrastructure and the associated applications. As soon as an integrative solution is in place that provides this information, the transition should be implemented and passed on to the central ITSM tool.

As mentioned previously under Organizational Prerequisites, the decision as to which environment the central tool runs in is dictated by the existing landscape. This should be re-examined from time to time however, as the number of cloud applications in relation to the number of on-premise applications is subject to change, as are the available features.

There is no single standard SAP strategy for this at present. Certain cloud products have an integrated incident management solution (C4C for example).

- Cloud – Cloud
  For cloud-to-cloud integration, the incident management tool of choice is a cloud solution
- On-Premise – Cloud
  With this constellation, on-premise tools are at the forefront. Effort should be undertaken to establish whether both worlds can be integrated.

Incident Management Requirements Faced by SAP

- Standardized incident management for all SAP cloud products and additional APIs for the connection of on-premise ITSM tools
- Provision of a function equivalent to the feedback function on-premise, which can be used to automatically provide all information required in the incident.

Hidden Costs

- It is necessary to develop an internal tool or to create manual tickets, thus necessitating effort on the part of the IT team
- Manual tickets are not properly qualified (information missing due to not being generated automatically). This results in extra effort when processing tickets.

7.4 Test Management

Many companies have implemented automated testing, for regression testing for example.

- Cloud – Cloud: Automated test management with WEB-IDE is already possible, but there is no integration with on-premise tools.
- On-Premise – Cloud: No integrative tool is available right now. The tests have to be aligned with each other. It is planned for CALM to incorporate this function in future.

7.4.1 Tools

- CALM
  It is planned for Cloud ALM to provide test management for cloud and hybrid landscapes in future.
- Solution Manager
  SAP's on-premise customers can use SAP Solution Manager for test management.
- WEB-IDE
  Currently implementable for cloud applications.

Test Management Requirements Faced by SAP

- It must be possible to schedule automated tests after updates in the cloud.
- The on-premise test tools have to interact with WEB IDE and corresponding tools (CALM).

Hidden Costs

- Integration tests for hybrid scenarios must be coordinated manually. This generates extra costs.

7.4.2 Recommended Links for the Topic:

- CTS+
- SAP Cloud Platform Transport Management [
- Cloud Availability Center
- CALM

8 People

The path towards the hybrid world is a significant challenge for the company's workforce. Compared to a purely on-premise IT landscape, roles, work processes and communication all change dramatically. This requires a willingness to accept changes, something which does not come naturally for most people.

It should be news to nobody that the break-neck pace of technological progress and accompanying expansion of the SAP product portfolio will cause employees working with SAP applications to experience significant changes in their roles.

Initial discussions in the DSAG community took place already more than five years ago. As mentioned above, these led to the establishment of a project group, which published in 2016 published the DSAG guide "SAP Basis of Tomorrow". This guide provides a detailed description of how the "classic SAP Basis" tasks will change and how they can ideally be evolved.

The guide identifies seven ***seven fields of action***:

- Skills and Roles – Cloud and Supplier Management, Empowerment of the Technology Architect, Focus on Project Work,
- Marketing and Self-Image – Creating a Service Catalog, Regular Exchange with the CIO And Other Stakeholders, Renaming SAP Basis
- New Technologies and Innovation – Test and Innovation Laboratory, Proactive and Regular Training
- Organization in Change – Bringing the Infrastructure And Application Teams Closer Together (in the sense of DevOps), Virtual Expert Teams
- Standardization and Automation – Automation of Routine Tasks, Out-Tasking of Uncommon Tasks
- "Cloudability", Outsourcing & Out-Tasking – Appraisal of Usability for the Cloud, Use of Own Service Types
- IT Roadmap – Influence on Own IT Roadmap

At this stage we do not intend to reiterate the contents of the guide. All experiences and recommendations listed there remain valid at the current point in time. Every IT decision maker with regard to an SAP environment and with staff who work in this area should have read "SAP Basis of Tomorrow" (together with the accompanying Master's thesis).

Discussions on the topic of "People" have brought about a number of general additions and priorities with an eye toward the question of hybrid operation. We would like to describe these in this section.

8.1 Complexity

In the “marketing and sales world” it’s obviously not uncommon to hear promises that this or that cloud solution will make it “easier” to focus on “core competencies” or to be able to achieve this at a faster rate. These objectives are attainable in part at least, but the truth of the matter is: The solution in its entirety will become more complicated. A system starts to become more complicated precisely when the number of influencing factors increases. And this starts to occur as soon as your IT landscape goes hybrid. Complicatedness is not a problem in its own right of course, and every modern IT system is complex, SAP systems even more so. But all factors, no matter how many there are, are known and are manageable. For IT systems therefore a manual is available.

Looking at it this way, even the largest hybrid landscape is complicated but manageable. Taking this statement to its logical extreme, we could say: We have systems A, B, and C, then replace B with D (in the cloud) and add E to C (on a cloud platform), and hey presto our new landscape is ready. There is a manual (documentation) for everything, the functions are described, we integrate these systems and that’s it - we’re “in business”. Our new system is admittedly more complicated (due to having more factors), but we have gained new and/or improved features – “check”. At least this is how management might see it.

The “problem” for complicated systems however is people. Because now things will become complex. The difference between complexity and complicatedness is that complexity introduces a degree of unpredictability. This arises because not all influencing factors are known, and there is a correlation between these factors according to rules that are as yet unknown.

But why does complexity increase? Complicated systems are managed by people of course (meaning they build, maintain, and use these systems), and the more complicated the system, the more people you will need. Instead of manuals, complex systems have guides – “here we are”.

The complexity of a hybrid landscape therefore increases in step with the number of influencing factors it has, and thus the number of people involved. This is not restricted to your company’s employees of course. It also includes people who are involved with the “cloud parts” of your hybrid landscape.

What consequences does this have? The amount of communication increases. At the same time, the high level of complexity necessitates a significant degree of structured mental effort. And this amounts to a contradiction, which represents a considerable challenge for today’s IT employees.

8.2 Communication and “Gamification”

Communication and interaction: In a hybrid landscape, communication increases above and beyond the technical communication between systems. This kind of communication increases significantly too of course, and we have already discussed the associated challenges, but what is meant here is communication and interaction between people.

Something that arose frequently in the discussions was that one of the drivers towards hybrid landscapes is the LOBs who require new applications faster, together with the fact that these LOBs thus have to be far more heavily involved. If you’d like to take another look at Cloud Onboarding Team to see which internal stakeholders are involved in the introduction of a cloud service, you’ll recognize just how much communication is required. And this continues of course after the service goes live.

There is absolutely no doubting that communication is one of the key competencies in the 21st century. This does not simply mean “expressing yourself clearly and understandably“ however. Rather, it means being able to receive, process and send a large number of messages, both synchronously and asynchronously, via a plethora of services and media, including as e-mail, various messengers, telephone, meetings, documents, wikis and social media platforms (including intra-company platforms, like SAP Jam).

At this point we would like to highlight another topic that is closely related to communication, at least in light of the neuro-chemical workings of the human brain. During the last few years, the concept of “gamification” has gained prominence in the corporate world. The definition of this concept according to Wikipedia is as follows: “…the application of characteristics of game elements in a non-game context… These game-like elements include points, high scores, performance graphs, leader boards, virtual possessions or badges”. Basically therefore it is a means of increasing motivation by stimulating the human reward system. The same thing also occurs during communication, especially social forms of communication, such as chats.

The problem with the reward system however is that once conditioned it demands further stimulation and thus displays a certain addictive character.

We certainly don’t intend to start delving into the much talked out differences between generations X, Y and Z. The fact is though that the younger generation in the workforce (not just the under 40s) has grown up with games and has been subject to a kind of “training” by them. It’s little wonder then that the gaming industry beats the music and film industry hands down in every metric. Which in turn provides an eloquent explanation for the gamification trend.

Note that this is not meant to be negative or critical. It’s an established fact that gaming improves the ability to rapidly process and react to a large number of inputs. It therefore also helps during communication - in particular while processing a lot of communication at once - and when events make it necessary to react quickly and decisively. From a scientific point of view, computer games have many positive aspects in terms of human key competencies in the 21st century.

There is the other side of the coin though. Once a reward system of this kind has become established, and users are accustomed to a continuous stream of stimulation, they can be somewhat thrown off course when confronted with the high-level of concentration required when learning about or expanding their knowledge of a complex topic. Or to put it more bluntly: It results in something that in itself is nothing new, but which has been the subject of frequent discussion over the last few years: procrastination. In other words, putting off activities for ever and a day in order to concentrate on simpler and/or quicker activities. Everybody has experienced this: „… I'll just send off a quick reply to this e-mail…, no point starting anything more demanding now - we've got a coffee break in 20 minutes…, think I'll take a look at this news article on our website first, might be interesting…". Wikipedia has the following to say: "This disorder is especially prevalent in people who for the most part work autonomously.". This is precisely what is expected in the modern workplace however: to be autonomous, independent, self-determined.

One thing we would like to stress of course is this: Although the experiences and trends discussed here might sound like sweeping generalizations, we recognize that everybody is unique.

8.3 Speed and Volatility

Everybody in the IT industry (and beyond) complains about the ever quickening pace they experience in the workplace. And just about every keynote speech these days features the famous hockey stick curve at some point. This is something we have all heard before: "Look at how things are developing… the car, the phone, the iPhone, Pokemon Go – amazing!" It's actually quite comical. And noticeably these curves always but always illustrate developments related to consumer products. These exponential growth rates are an obvious result of the global connection and the sheer number of consumers and their disposable income. When it comes to products and service for companies though, things look a little different. Which IT company doesn't dream of this kind of growth? With its cloud products, SAP is no exception. In companies, it's logical that new products, solutions and services come up against structures, and that this puts limits on the speed of adoption.

Growth and speed naturally have consequences for all companies, as there is always a direct or indirect end customer at the end of the chain. This increases the pressure on the internal IT team to act quickly and to meet expectations. This results in something that all IT team workers notice these days: an ever-increasing number of projects, paired with permanent pressure to change and to adapt. Today's (and tomorrow's) IT workers are in virtually permanent project mode, and are normally involved in several projects at once.

The increasing speed leads to another problem, which by its very nature is something most people are troubled by: volatility. This phenomenon can be summed by the words “moving target”, and is the result of a number of factors:

- Requirements changing within a project.
- Framework conditions changing during the course of a project.
- The more complicated systems are, the more difficult and costly the specifications are for the desired final status, which results in compromises being made.

There are of course requirements and framework conditions that work against this. Examples of this are compliance, rules and certification requirements in critical domains (medicine, traffic and so on). These of course all cost time and money, and increase the “inner tension” between requirements and feasibility within the company.

The answer to “speed and volatility” is - who’d have thought it? – Agility, in other words the flexibility or nimbleness of organizations and/or people in structures and/or processes. Which has been a huge concern in the IT world over the last few years. We’ve all heard the terms development, DevOps, scrum and so on. But adapting the company’s IT to these new methods in order to better prepare it for the challenges is a huge task. A bit of scrum doesn’t work - it’s all or nothing.

This means that employees have to be open to change and be able to adapt. The question of Change Management in organizations never ends, but it is one that has to be met head on.

8.4 Focus and Self Organization

If we take a look at the working environment of today's IT workers, it becomes obvious that the main personal challenge for them is switching between work that demands a high level of communication and work that demands a high level of concentration.

Switching to the former is something that most people find quite straightforward, as humans are a communicative species, and we need little encouragement to communicate. Switching to work that demands a high level of concentration is a genuine challenge however, and one that demands focus and organization.

At this point we do not intend to go into any more detail about focus. This is a very individual challenge that is covered already by a plethora of guidebooks providing techniques for improving focus, concentration and so on.

Self organization, or more to the point effective self organization on the part of employees is extremely important in order to successfully meet the challenges outlined above. You might well counter that this is nothing new and that this has always been the case. You will probably also maintain that working in a structured manner is generally more successful. Due to the challenges mentioned above however (complexity, rate of change, communication and so on) it is more essential now than ever before that the member of an organization or department possess a high degree of self organization.

Everybody working in IT today is their own multi-project manager!

If employees do not possess a sufficient degree of self-organization, they will find it hard to assert space for themselves and thus to free themselves up to work in a focused manner and with a high level of concentration on complicated systems or complex problems. You probably know - or at least know of - colleagues who don't seem to achieve anything on their own and who always have to be told what to do, in other words who require micro-management. Strangely these are often colleagues who react to e-mails immediately or who always have time whenever somebody asks for help at short notice (which can be an advantage in fact!).

Every management guidebook on the market will tell you that micro-management is completely outdated and should be avoided. The future belongs to autonomous and self-organized employees and teams. The truth of the matter however is that this requires certain abilities. And not everybody has these or is able to develop them. To avoid any misunderstanding, this is without doubt the right (and indeed the only) path for the future, but it is far from easy!

8.5 Training

Once you begin to integrate cloud applications into your landscape, when hybrid operation begins that is, an obvious question is which training measures to adopt.

In this section, we describe not so much the technical challenges as the personal challenges. Of course however, the technical knowledge of the employees is the absolute foundation for a successful project or successful hybrid operation. If you are about to embark on this type of project therefore, you should schedule the relevant training measures for the solutions to be integrated. Any other course of action would be negligent. For many SAP cloud offerings, training courses are provided that deal with integration with on-premise solutions. These can provide valuable support.

You should base the training measures you adopt on the new role concept that is described in the DSAG guide “SAP Basis of Tomorrow”. You should focus on more than just the actual cloud application that is at the heart of your project however. A particularly important role here is that of technology architects, and you need to invest accordingly in this particular expertise. Ideally, your HR team will already have a concept and a strategy for the individual development of your employees. In this case, you should use this in order to gradually establish the news roles in the team.

In addition to technical aspects, the soft skills mentioned in this section are crucial for success in the hybrid future and particularly of course in hybrid operation. What could be more obvious than including training measures for these too? It’s obvious of course that you won’t get very far with requests like this. If you put forward a project plan for the introduction of a cloud solution including hybrid operation, and schedule a training measure for self-organization, you are unlikely to be successful. And this is understandable, as these abilities are not project-specific. So what you need here is the HR department, who you should make aware of the challenges that your IT employees are going to be faced with. The alternative to this is simply taking on more staff or replacing current employees with others who have the right abilities. Which is a difficult and/or expensive undertaking, especially with the lack of qualified specialists on the job market.

It should also not be forgotten that employees need to be freed up to pursue training activities. As logical as this might seem, experience shows that this is often in short supply these days. The high level of pressure from daily work and collaboration in projects makes this even more difficult.

To make this clear: Acquiring knowledge, which of course is the whole point of training measures, is something that demands a high level of concentration, but not of communication. Gaining new knowledge demands significant effort, and this will not come about if people are distracted by e-mails or other forms of communication. This is another way in which people need to be freed up.

8.6 Conclusion

To round off this somewhat unconventional section, we would like once more to draw your attention to the DSAG guide “SAP Basis of Tomorrow“. Please take the time to read this guide.

In our opinion, the key to successful hybrid operation is the people, the employees. They must be able to overcome the challenges involved. To do this, they require support by being freed up to acquire new information and need to be motivated by being provided with both hard skill and soft skill training, as well as recognition for their achievements.

People Requirements Faced by SAP

No Hidden Costs

- At best, operating a hybrid landscape is cost-neutral. Compared to purely on-premise operation it is generally more expensive, as it is more complicated, more complex and engenders new and additional requirements.
- If employees cannot or will not commit themselves fully to the operation of a hybrid IT solution, they need additional resources with the corresponding skills.

APPENDIX

Glossary

General Terms – Abbreviations	
Capex	Capital expenditure
CSA	Cloud Controls Matrix
DMZ	Demilitarized zone
E2E-BPM	End-To-End Business Process Monitoring
IAM	Identity and Access Management
IDM	Identity Management
ITSM	IT Service Management
Opex	Operational expenditure
SAML	Security Assertion Markup Language
SOC	PAN Auditing Procedure for Data Protection
SSO	Single Sign-On
UXMon	User Experience Monitoring

APPENDIX A: SAP Service Catalog

Release Order 01 SAP Operation Services – Change Catalog

Document Version	
Document Date	

Preamble	The "Change Catalog" document does not supersede or replace any of the contractually agreed SOW's. Purpose of the document is to explain and detail some of the contractual areas which are complex to understand. The document is NOT a contractual document, the eventual reference for all Service scope questions are the Contract SOW's.

Document structure	Column/Cell	Description
	Sec.	Sec. = Section: Level 1 ordering structure
	ID	Level 2 Ordering Structure; Sec. + ID is unique Identifier
	Agreed by Date	Date of agreement
	Service Area Service Sub Area Service Description	Description of Service and Sub-Service Area and short description of respective Service
	A Responsibility Customer Responsibility	X in respective column explains whether A or Customer is responsible for respective Service Item.
	Included	Determines whether this action is included in the base fee or not (=extra order)

Document History	Date	Update

Document Authors

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
1	0	SAP system administration	**SAP SYSTEM ADMINISTRATION**			
1	1	SAP system administration	In general all Activities in client 000, DB and OS	X		yes
1	2	SAP system administration	In general all Activities in productive client		X	no
1	3	SAP system administration	Maintain clustering environment (OS, clustering tool, SAP specific parameters) according to VENDOR standards on CUSTOMER database servers	X		yes
1	4	SAP system administration	Periodically test the cluster fail-over mode	X		yes
1	5	SAP system administration	Start/stop SAP system instances when needed	X		yes
1	6	SAP system administration	**Maintain Operating System**			
1	7	SAP system administration	Define and implement to correct, change or improve current settings	X		yes
1	8	SAP system administration	Restart OS according to OS or SAP system needs	X		yes
1	9	SAP system administration	Plan and implement the update of Operating System corrections and Upgrades following VENDOR recommended approach	X		yes
1	10	SAP system administration	**Maintain SAP System Landscape**			
1	11	SAP system administration	Define needs in order to change or improve the existing landscape according to Solution Design		X	no
1	12	SAP system administration	Review request for change and adapt the existing landscape according to Solution Design	X		yes
1	13	SAP system administration	Create and maintain SAP Basis operation management procedures	X		yes
1	14	SAP system administration	**Maintain SAP system parameters, SAP system Change Option, SAP system profiles, SAP Operation Modes and Instances, according to specification from the CUSTOMER**			
1	15	SAP system administration	Define needs in order to correct, change or improve current setting		X	no
1	16	SAP system administration	Review request for change and implement changes	X		yes
1	17	SAP system administration	**Maintain workload distribution (focus on load balancing) in cooperation with customer; SAP Web Dispatcher etc.**			
1	18	SAP system administration	Define needs in order to correct, change or improve current setting		X	no
1	19	SAP system administration	Review request for change and implement changes	X		yes
1	20	SAP system administration	**Maintain workload distribution (focus on load balancing) in cooperation with customer; Logon Load Balancing, Logon Groups**			
1	21	SAP system administration	Plan and define SAP Logon Groups and Operation Modes		X	no

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
1	22	SAP system administration	Initial setup of Logon Groups and RFC server Groups	X		yes
1	23	SAP system administration	Maintain Logon Groups, RFC server Groups and operation Modes during Maintenances	X		yes
1	24	SAP system administration	Maintain Logon Groups, RFC server groups and operation Modes for long term normal operation		X	no
1	25	SAP system administration	Maintain customer system clients and client parameters		X	no
1	26	SAP system administration	Maintain SAP system client 000 and client parameters, maintain SAP system client 066 and client parameters when applicable (transaction SCC4)	X		yes
1	27	SAP system administration	Maintain schedule of Early Watch Alert reports, define system landscape in Solution Manager	X		yes
1	28	SAP system administration	**Review and act on errors of Early Watch Alerts**			
1	29	SAP system administration	Analyze recommendations and propose implementation	X	X	yes
1	30	SAP system administration	Review, plan implementation and approve	X	X	yes
1	31	SAP system administration	Implement	X	X	yes
1	32	SAP system administration	**Implement SAP application tuning recommendations from SAP services excluding weekly Early Watch alert**			
1	33	SAP system administration	Analyze recommendations and propose implementation		X	no
1	34	SAP system administration	Review, plan implementation and approve		X	no
1	35	SAP system administration	Implement		X	no
1	36	SAP system administration	**Implement SAP basis tuning recommendations from SAP services excluding weekly Early Watch alert**			
1	37	SAP system administration	Analyze recommendations and propose implementation	X		yes
1	38	SAP system administration	Review, plan implementation and approve		X	no
1	39	SAP system administration	Implement	X		yes
1	40	SAP system administration	Perform SAP system copy (not client copy): Refresh system e.g. development/test/sandbox from other SAP systems based on CUSTOMER input	X		no
1	41	SAP system administration	Perform SAP client copy: Copy client within a SAP system or from remote based on CUSTOMER input	X		no
1	42	SAP system administration	Open OSS connection for production client and maintain logon details for SAP experts when needed	X		yes
1	43	SAP system administration	Schedule, release, maintain and monitor SAP standard maintenance batch jobs according to SAP recommendations and CUSTOMER needs	X		yes

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
1	44	SAP system administration	Schedule, setup, release, maintain CUSTOMER application batch jobs according to specification from Application teams and SAP requirements, Test in test environment prior to setup in production		X	no
1	45	SAP system administration	Define and maintain notification/escalation procedures for CUSTOMER application batch jobs.		X	no
1	46	SAP system administration	Handle job aborts, either batch or dialog	X		yes
1	47	SAP system administration	**Perfomance Analysis**			
1	48	SAP system administration	Performance analysis after recognition of bottlenecks	X		no
1	49	SAP system administration	Performance analysis after recognition of bottlenecks that affect the agreed SLA	X		yes
1	50	SAP system administration	Assist external consultants (e.g. SAP engineers) in relevant questions e.g. performance, job scheduling, transport of objects	X		no
1	51	SAP system administration	Application performance analysis, tuning and optimization		X	no
1	52	SAP system administration	Assist external application consultants in relevant questions e.g. performance, job scheduling, transport of objects.		X	no
1	53	SAP system administration	Maintain SAP router based on customer input	X		yes
1	54	SAP system administration	**Printing and Output Managament**			
1	55	SAP system administration	Overall Printing Management		X	no
1	56	SAP system administration	Manage SAP print and spool subsystem such as SAP spool administration	X		yes
1	57	SAP system administration	Define, change or delete output devices in SAP systems	X		yes
1	58	SAP system administration	Deliver according printer documentation and drivers		X	no
1	59	SAP system administration	Maintain printer OS queues on service provider-maintained hosts	X		yes
1	60	SAP system administration	Maintain printer OS queues on customer-maintained hosts		X	no
1	61	SAP system administration	Manage SAP system user accounts in accordance with security policies		X	no
1	62	SAP system administration	Manage SAP end user accounts in accordance with security policies		X	no
1	63	SAP system administration	Manage SAP end user accounts password reset in accordance with security requirements.	X		yes
1	64	SAP system administration	Manage Service Provider Users in client 000, 066	X		yes
1	65	SAP system administration	Manage OS system user accounts and password	X		yes
1	66	SAP system administration	Maintain customer accounts for FTP, SFTP or NFS, Samba shares, incl. creation of new shares	X		no

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
1	67	SAP system administration	Administration of SAP end-user master record, roles, authorizations and profiles following CUSTOMER procedures and SAP Security Guides. This will be performed by the Roles and Authorizations team		X	no
1	68	SAP system administration	Manage SAP OSS customer user accounts and developer and object keys		X	no
1	69	SAP system administration	Maintain SAP OSS Service Provider user account	X		yes
1	70	SAP system administration	**Perform backup, restore and recovery of SAP systems and databases**			
1	71	SAP system administration	Perform regular backup in accordance with agreed service parameters, perform restore due to system failure or data corruption caused by technical or software defect, perform regular restore tests for production system components on a yearly basis in accordance with agreed service parameters	X		yes
1	72	SAP system administration	Perform ad hoc extra backup on CUSTOMER request, perform restore on CUSTOMER request (authorized requestors)	X		yes
1	73	SAP system administration	Maintain Transport Management System Infrastructure (e.g. File System, NFS mounts)	X		yes
1	74	SAP system administration	Maintain SAP Transport Management System		X	no
1	75	SAP system administration	Transport of SAP objects		X	no
1	76	SAP system administration	Handle issues during transport with return code > 8	X		yes
1	77	SAP system administration	Maintain and configure Java/Portal Content		X	no
1	78	SAP system administration	Transport Java/Portal objects		X	no
1	79	SAP system administration	**Language Installation and Maintenance**			
1	80	SAP system administration	Provide language installation files based on customer request	X		yes
1	81	SAP system administration	Adapt profile parameters for language selection based on customer request	X		yes
1	82	SAP system administration	Import new languages	X		no
1	83	SAP system administration	Plan Downtimes	X	X	yes
1	84	SAP system administration	Communicate scheduled downtimes, customer information or other planned maintenances based on changes to customer end users		X	no
1	85	SAP system administration	Capacity reporting and planning based on Service Provider Standard Reports	X		yes
1	86	SAP system administration	Management of SAP contracts and relationship to SAP AG		X	no
1	87	SAP system administration	Support CUSTOMER during Audits, e.g. provide information, describe processes, run scripts	X		no
1	88	SAP system administration	Follow operational ITIL Functions: Incident Management, Change Management, Problem Management	X	X	yes

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
2	0	SAP software corrections and upgrade	**SAP SOFTWARE CORRECTIONS AND UPGRADE**			
2	1	SAP software corrections and upgrade	Review available Country Legal Changes and Support Packages for potential resolution to SAP issues in CUSTOMER SAP solutions. Analyze consequences/impact, recommend implementation approach.		X	no
2	2	SAP software corrections and upgrade	**Implement software corrections (Kernel-Patches, Hot Fixes and Support Packages/Stacks) across the system landscape and in accordance with CUSTOMER change and release to production processes**			
2	3	SAP software corrections and upgrade	Plan update of software corrections following VENDOR recommended approach		X	no
2	4	SAP software corrections and upgrade	Perform preparation activities (e.g. lock user accounts, stop background jobs, stop interfaces)		X	no
2	5	SAP software corrections and upgrade	Install Kernel Patches and Hot Fixes following SAP requirements and recommendations	X		yes
2	6	SAP software corrections and upgrade	Install software corrections (Support Packages/Stacks) via SPAM/SAINT following SAP requirements and recommendations	X		yes
2	7	SAP software corrections and upgrade	Install software corrections (Support Packages/Stacks) via SUM following SAP requirements and recommendations	X		no
2	8	SAP software corrections and Upgrade	Perform modification adjustments (SPAU, SPDD)		X	no
2	9	SAP software corrections and upgrade	Initiate Business Application testing		X	no
2	10	SAP software corrections and upgrade	Connection test to SAP components (e.g. BIA, pre Calculation Server, TREX, Easy Archive)	X		yes/no
2	11	SAP software corrections and upgrade	Perform Interface Tests		X	no
2	12	SAP software corrections and upgrade	Schedule downtime following CUSTOMER business requirements	X	X	yes
2	13	SAP software corrections and upgrade	Perform post-install activities e.g. unlock user accounts, re-start background jobs, re-start interfaces)		X	no
2	14	SAP software corrections and upgrade	Review available OSS notes for potential implementation and/or resolution to SAP issues in CUSTOMER SAP solutions. Analyze consequences/impact, recommend implementation approach.	X	X	yes
2	15	SAP software corrections and upgrade	**Implement OSS notes across the system landscape in accordance with CUSTOMER change and release to production processes**			
2	16	SAP software corrections and upgrade	Plan implementation of OSS notes		X	no

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
2	17	SAP software corrections and upgrade	Check prerequisites and implement OSS notes following SAP requirements		X	no
2	18	SAP software corrections and upgrade	Correct Side Effect of notes		X	no
2	19	SAP software corrections and upgrade	Initiate request for application testing		X	no
2	20	SAP software corrections and upgrade	Deploy software packages from third-party providers (e.g. job scheduling software, Vistex, FIS, PBS) following change management process	X		no
2	21	SAP software corrections and upgrade	Review available Enhancement Packages or new software releases for potential implementation of new functionality		X	no
2	22	SAP software corrections and upgrade	**Implement Enhancement Packages or new software releases across the system landscape in accordance with CUSTOMER change and release to production processes**			
2	23	SAP software corrections and upgrade	Plan implementation of Enhancement Packages or new software releases in cooperation with business process owners		X	no
2	24	SAP software corrections and upgrade	Check prerequisites and install Enhancement Package or new software releases following SAP requirements and recommendations.	X		no
2	25	SAP software corrections and upgrade	Perform preparation activities e.g. lock user accounts, stop background jobs, stop interfaces)		X	no
2	26	SAP software corrections and upgrade	Activate relevant business functions		X	no
2	27	SAP software corrections and upgrade	Perform modification adjustments (SPAU, SPDD)		X	no
2	28	SAP software corrections and upgrade	Initiate for application testing		X	no
2	29	SAP software corrections and upgrade	Connection test to SAP components (e.g. BIA, pre Calculation Server, TREX, Easy Archive)	X		no
2	30	SAP software corrections and upgrade	Perform Interface Tests		X	no
2	31	SAP software corrections and upgrade	Schedule downtime following CUSTOMER business requirements	X	X	no
2	32	SAP software corrections and upgrade	Perform post-install activities e.g. unlock user accounts, re-start background jobs, re-start interfaces)		X	no
2	33	SAP software corrections and upgrade	Verification and implementation of SAP kernel patches	X		no
2	34	SAP software corrections and upgrade	SAP GUI or any activity that belongs to it will be defined in upcoming versions of this document			no
3	0	SAP system monitoring	**SAP SYSTEM MONITORING**			

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
3	1	SAP system monitoring	Set up, install, configure and test monitoring environment and tools used by Service Provider	X		yes
3	2	SAP system monitoring	Set up, configure and test monitoring of customer special needs (e.g. SAP Solution Manager, critical business process chain)		X	no
3	3	SAP system monitoring	Configure monitoring tools, set thresholds and values and subsequent events, alerts that will be generated when/if one of the thresholds is exceeded	X		yes
3	4	SAP system monitoring	Manage monitoring agents in all SAP systems that are in scope	X		yes
3	5	SAP system monitoring	Review event and alert thresholds regularly to ensure appropriateness and accuracy	X		yes
3	6	SAP system monitoring	Respond to events following the notification/escalation procedure	X		yes
3	7	SAP system monitoring	Monitor status of CUSTOMER application batch jobs and follow the notification/escalation procedures	X	X	yes
3	8	SAP system monitoring	Monitor SAP standard maintenance batch jobs	X		yes
3	9	SAP system monitoring	Monitor qRFC queues (outbound and inbound) e.g. data transfer between the ERP back-end system and the CRM server (setup of additional/special monitoring handled as small project)	X		yes
3	10	SAP system monitoring	Monitor password security policies on OS, DB level	X		yes
3	11	SAP system monitoring	Monitor password security policies on SAP internal level		X	no
4	0	SAP system setup	**SAP SYSTEM SETUP**			
4	1	SAP system setup	Plan and define: system landscape, customer system clients, client parameters, system Change Option, Operation Modes and Instances, connections to other SAP systems		X	no
4	2	SAP system setup	Define SAP system sizing based on input from CUSTOMER	X		no
4	3	SAP system setup	Design and implement system infrastructure and required hardware	X		no
4	4	SAP system setup	Install SAP and database software	X		no
4	5	SAP system setup	Install and configure clustering environment (OS, clustering tool, SAP-specific parameters) in accordance with VENDOR standards	X		no
4	6	SAP system setup	Set up high availability solution for SAP system instances selected by CUSTOMER	X		no
4	7	SAP system setup	Create CUSTOMER SAP system clients, set up clients parameters in accordance with CUSTOMER specifications	X		no
4	8	SAP system setup	Set up SAP system Change Option in accordance with CUSTOMER specifications (transaction SCC4)		X	no
4	9	SAP system setup	Define and set up SAP system parameters, SAP system profiles in cooperation with CUSTOMER and Service Provider Standard recommendations	X		no
4	10	SAP system setup	Create SAP Remote Function Calls connections		X	no

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
4	11	SAP system setup	Configure SAP Transport Management System		X	no
4	12	SAP system setup	Deploy Add-Ons	X		no
4	13	SAP system setup	Define and set up workload distribution Logon Load Balancing, SAP Logon Groups		X	no
4	14	SAP system setup	Set up workload distribution on SAP Web Dispatcher	X		yes
4	15	SAP system setup	Define and set up SAP Operation Modes and Instances	X		yes
4	16	SAP system setup	Connect system to SAP Solution Manager and SAP System Landscape Directory	X		no
4	17	SAP system setup	Enable SAP Early Watch Alert reporting in CUSTOMER Solution Manager	X		no
4	18	SAP system setup	Set up and enable Service Provider Standard monitoring of the system(s)	X		no
4	19	SAP system setup	Set up and enable backup	X		no
4	20	SAP system setup	Develop and maintain documentation e.g. System Landscape (hardware view), High Availability, Backup, Operational Manual	X		no
4	21	SAP system setup	Develop and maintain documentation e.g. System Landscape (logical view), System customer clients, Transport Procedures, Instructions to Service Provider regarding special requirements for system setup		X	no
5	0	Database administration	**DATABASE ADMINISTRATION**			
5	1	Database administration	Install and configure the database clustering environment (OS, clustering tool, database specific parameters) in accordance with VENDOR standards on database servers	X		no
5	2	Database administration	Periodically test the cluster fail-over	X		yes
5	3	Database administration	Notify Service Provider about any specific tasks that should be completed in the case of a fail-over switch (e.g. system restart of connected systems)		X	no
5	4	Database administration	Configure database parameters for application performance based on requirements from CUSTOMER	X		yes
5	5	Database administration	Manage the file structure (for example, data files, log files, and so on)	X		yes
5	6	Database administration	Manage the storage space for the database on the storage subsystem	X		yes
5	7	Database administration	Start/stop database	X		yes
5	8	Database administration	Adapt database parameters required to maintain the agreed service levels	X		yes
5	9	Database administration	Perform database system management	X		yes
5	10	Database administration	Create and maintain database operation management procedures	X		yes
5	11	Database administration	**Perform backup, restore and recovery of SAP systems and databases**			

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
5	12	Database administration	Setup, document, execute and verify the data backup	X		yes
5	13	Database administration	Perform regular backup according to agreed service level	X		yes
5	14	Database administration	Perform restore due to system failure or data corruption caused by technical or software defect	X		no
5	15	Database administration	Perform regular restore tests for production system components	X		no
5	16	Database administration	Perform ad hoc extra backup on CUSTOMER request, perform restore on CUSTOMER request (authorized requestors)	X		yes
5	17	Database administration	Define authorized key users which are allowed to request database restores		X	no
5	18	Database administration	Provide information about non-regular data imports and database growth (e.g. SAP rollout)		X	no
5	19	Database administration	**Perfomance Analysis**			
5	20	Database administration	Perform database performance troubleshooting	X		yes
5	21	Database administration	Database performance tuning at system level (performance ratios, I/O load balancing, database buffers and utilization of memory), apply changes in accordance with CUSTOMER change and release to production processes	X		no
5	22	Database administration	Database performance tuning at application level (for example, SQL Query optimization, global performance due to application development/update)		X	no
5	23	Database administration	Manage network access to remote databases (listeners, SQL hosts).	X		no
5	24	Database administration	Maintain CUSTOMER own data/procedures (schema, business/application data, associated indexes etc.).		X	no
5	25	Database administration	Communicates scheduled downtimes to CUSTOMER end-users and Service Provider		X	no
5	26	Database administration	Creation, deletion of database objects (indexes, tables) on request following change management procedure	X		no
5	27	Database administration	Supporting CUSTOMER during audits, for example by providing information, describing processes, running scripts	X		no
6	0	Database monitoring	**DATABASE MONITORING**			
6	1	Database monitoring	Set up, install, configure and test monitoring environment and tools	X		yes
6	2	Database monitoring	Configure monitoring tools, set thresholds and values and subsequent events that will be generated when/if one of the thresholds is exceeded	X		yes
6	3	Database monitoring	Define alerts for availability, capacity, disk utilization	X		yes
6	4	Database monitoring	Review monitored event thresholds regularly to ensure appropriateness and accuracy	X		yes

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
6	5	Database monitoring	Respond to events following the notification/escalation procedure	X		yes
6	6	Database monitoring	Monitor the database growth and increase database size accordingly.	X		yes
7	0	Database software corrections and upgrade	**DATABASE SOFTWARE CORRECTIONS AND UPGRADE**			
7	1	Database software corrections and upgrade	Review available software corrections (patches, hot fixes) or new software versions for potential implementation and/or resolution to database issues in CUSTOMER SAP solutions. Analyze consequences/impact, recommend implementation approach.	X		yes
7	2	Database software corrections and upgrade	**Upgrade or patch database with the latest recommended patch level from the database vendor, in accordance with CUSTOMER change and release to production processes**			
7	3	Database software corrections and upgrade	Decide to update of software corrections (patches, hot fixes) or new software versions following VENDOR recommended approach	X		yes
7	4	Database software corrections and upgrade	Perform preparation activities e.g. lock user accounts, stop background jobs, stop interfaces)		X	no
7	5	Database software corrections and upgrade	Install software corrections (patches, hot fixes) following database vendor and SAP requirements	X		yes
7	6	Database software corrections and upgrade	Upgrade Database software (release change)	X		no
7	7	Database software corrections and upgrade	Schedule downtime following CUSTOMER business requirements	X	X	yes
8	0	Database reorganizations	**DATABASE REORGANIZATIONS**			
8	1	Database reorganizations	Identify database objects that need to be reorganized.		X	no
8	2	Database reorganizations	Review VENDOR recommendations, plan reorganization of database		X	no
8	3	Database reorganizations	Schedule downtime for database or database objects export/import		X	no
8	4	Database reorganizations	Communicates scheduled downtimes to CUSTOMER end-users and Service Provider		X	no
8	5	Database reorganizations	Perform reorganization of database or selected database objects on request	X		no
9	0	Database security	**DATABASE SECURITY**			
9	1	Database security	Change passwords for all database administrator users in accordance with security policies	X		yes
9	2	Database security	**Implement security standards and install software changes to overcome known security weaknesses**			
9	3	Database security	Patch known critical database vulnerabilities	X		yes
9	4	Database security	Patch database software infrastructure component vulnerabilities (database engine, listener)	X		yes

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
9	5	Database security	Notify about changes to security policies or any discovered security leaks	X	X	yes
10	0	HANA Special Add-Ons	HANA SPECIAL ADDONS			
10	1	Database software corrections and upgrade	HANA - Update and patching the OS - Deployment of new image (OS update installations for SLES)	X		no
10	2	Database software corrections and upgrade	HANA - Update and patching the OS - Patching of OS components	X		yes
10	3	Database software corrections and upgrade	HANA - Update and Patching SAP HANA Database Software (Revision Update)	X		yes
10	4	Database software corrections and upgrade	HANA - Update and patching file systems components	X		yes
10	5	Database software corrections and upgrade	HANA - Update and Patching Storage Components	X		yes
10	6	SAP system administration	HANA System Copy	X		no
10	7	SAP system setup	HANA Solution Sizing based on input from CUSTOMER	X		no
10	8	SAP system setup	Installation of new HANA DB and if necessary migration from previous DB System	X		no
11	0	Solution Manager Add-Ons	SOLUTION MANAGER ADDONS			
11	1	Preparation	Review and establish SLD concept	X		no
11	2	Preparation	Define technical and business system information for SLD		X	no
11	3	Preparation	Configure correct technical and business system information in SLD	X		no
11	4	Preparation	Establish User and Role Procedure for Users on Managed System		X	no
11	5	Installation	SAP Solution Manager Installation	X		no
11	6	Installation	Installation Post-Processing: SolMan Setup (Preparation and Basic Configuration)	X		no
11	7	Installation	SMD Agent Installation	X		no
11	8	Installation	Introscope Enterprise Manager Installation	X		no
11	9	Configuration	Managed System Configuration	X		no
11	10	Configuration	EWA	X		no
11	11	Configuration	Service Level reports	X		no
11	12	Configuration	System Monitoring (on customer request)	X		no
11	13	Configuration	MAImon including threshold adaptation	X		yes
11	14	Configuration	BEX Query	X		no
11	15	Operation	SolMan-related tasks when decommisioning a system	X		yes

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
11	16	Operation	SolMan-related tasks when patching a satellite system	X		yes
11	17	Operation	SolMan SPS patching Post Action	X		no
11	18	Operation	Update SLD CIM model/CR content	X		yes

Responsibility Matrix Key:

D	Responsible (D from the German “Durchführung”) – responsible for execution. The party or parties responsible for executing the activity/activities.
V	Accountable (V from the German “Verantwortlich”) – responsible in terms of “approving”. The party that assume the responsibility, in the legal or in the business sense.
M	Consulted (from the German “Mitwirkung”) – provides additional, mainly business-related information. The party or parties that will collaborate in the execution of the activity by providing additional, mainly business-related information.
I	Information – to be informed. The party or parties that will be informed about the progress or the result of the activity and is/are authorized to procure information as required.
F	Release – The party or parties whose approval is required before an activity can commence.
P	Project – Optional service, provision within the terms of the projects commissioned from the service provider.

APPENDIX B: SAP Service Parameter

B. SAP Basis Operation

B.1 Provision of Services

For services within the domain of SAP operation, the following completion times have been agreed for the provision of services.

Priority	Completion Time
Priority 1 (Critical)	8 h
Priority 2 (Major)	3 working days
Priority 3 (default)	10 working days
Priority 4 (request)	20 working days

Category Examples of Services:

Priority 1: Implementation of single SAP Note, setting up printers, recovery clone

Priority 2: Print server, authorization changes, creating transactions, job requirements and job changes

Priority 3: Creating test system, installation of SAP Add-On in development or text environment

Priority 4: Installation of a new SAP productive system, installation of hot packages, swap SAP kernel in entire landscape

During the transitional phase, the services are categorized.

B.2 System Availability

“Platinum” application availability for all productive SAP system landscapes (complete Landscape), including subcomponents (such as LiveCache or BWA)

“Bronze” application availability for all productive test SAP system landscapes (sandbox systems), including subcomponents (such as LiveCache or BWA)

“Platinum” application availability for all productive non-SAP components (such as MQ Series, Content Manager, Business Connector, Vertex, and Dollar Universe)

Maximum number of breakdowns allowed per year: See point 3. Data Center Services measuring criteria for system availability of SAP systems:

- Logon check in every system
- Update program must be active in every system

- Lock management must be in working order in every system

Measuring criteria for system availability of non-SAP systems:

- SAP interface must be in working order
- Individual check routines using tools, current status: SAP SolMan and/or Nagios depending on the system (for example Dollar Universe, MQ Series)

The SAP application server and database server are to be operated without specific service periods for standard system maintenance tasks (such as database and operating system patches, and SAP kernel upgrades). Implementation takes place in the customer default by means of failover mechanisms, without interruption of SAP operation.

B.3 Response Times

SAP response times are measured using the response time distribution (including dialog time) displayed in transaction ST03N. This considers the averaged monthly value of all instances using the cumulative percentage distribution. Of relevance here is the rate of transactions that attain a responsetime of <0.1s, <0.5s and <1s. For certain transaction types, the maximum hourly average during the online peak time is also considered. This is displayed in transaction ST03N in the time profile. The online peak time is the hour with the greatest number of transactions per transaction type per hour in the relevant system.

The average response times from the SAP systems are defined according to the following table. They reflect the current status of the systems plus a buffer of around 10%:

		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PG1	BACKGROUND	72.5	85.0	85.0	2500
PG1	DIALOG	55.0	82.5	90.0	700
PG1	RFC	42.5	70.0	85.0	1600
PG1	UPDATE	70.0	90.0	92.5	
PG1	UPDATE2	80.0	95.0	97.5	
		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PE1	BACKGROUND	75.0	87.5	90.0	3000
PE1	DIALOG	45.0	75.0	87.5	850
PE1	RFC	45.0	75.0	90.0	3000
PE1	UPDATE	50.0	80.0	87.5	
PE1	UPDATE2	60.0	90.0	95.0	

		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PA1	BACKGROUND	80.0	87.5	90.0	7500
PA1	DIALOG	35.0	65.0	80.0	900
PA1	RFC	35.0	65.0	80.0	3000
PA1	UPDATE	50.0	77.5	85.0	
PA1	UPDATE2	57.2	87.5	95.0	
		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PP1	BACKGROUND	82.5	90.0	95.0	800
PP1	DIALOG	40.0	58.5	72.5	1100
PP1	RFC	52.5	77.5	85.0	650
PP1	UPDATE	52.5	80.0	90.0	
PP1	UPDATE2	70.0	95.0	97.5	
		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PM1	BACKGROUND	75.0	90.0	92.5	2000
PM1	DIALOG	40.0	70.0	80.0	1100
PM1	RFC	70.0	80.0	90.0	800
PM1	UPDATE	42.5	75.0	85.0	
PM1	UPDATE2	60.0	90.0	95.0	
		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PC1	BACKGROUND	80.0	92.5	95.0	
PC1	DIALOG	57.5	80.0	90.0	
PC1	RFC	10.0	37.5	70.0	1100
PC1	UPDATE	50.0	95.0	97.5	
PC1	UPDATE2	0.0	90.0	95.0	
		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PO1	BACKGROUND	70.0	85.0	90.0	1100
PO1	DIALOG	40.0	67.5	77.5	1300
PO1	RFC	27.5	70.0	85.0	700
PO1	UPDATE	80.0	95.0	97.5	
PO1	UPDATE2	65.0	82.5	90.0	
		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PW1	BACKGROUND	60.0	70.0	75.0	22000
PW1	DIALOG	42.5	65.0	75.0	2800
PW1	HTTP	85.0	90.0	92.5	650
PW1	RFC	40.0	65.0	80.0	3000

		< 0.1s	< 0.5s	< 1s	Peak Response Time AVG (ms)
PH1	BACKGROUND	65.0	90.0	92.5	
PH1	DIALOG	72.5	87.5	92.5	650
PH1	RFC	25.0	50.0	95.0	350
PH1	UPDATE	65.0	90.0	95.0	
PH1	UPDATE2	85.0	95.0	97.5	
		< 0.1s	**< 0.5s**	**< 1s**	**Peak Response Time AVG (ms)**
PH2	BACKGROUND	57.2	80.0	85.0	1600
PH2	RFC	25.0	60.0	80.0	800
		< 0.1s	**< 0.5s**	**< 1s**	**Peak Response Time AVG (ms)**
PR1	BACKGROUND	57.5	85.0	90.0	18000
PR1	DIALOG	30.0	65.0	75.0	850
PR1	RFC	57.5	60.0	90.0	450

If these response times are not met in a given month, analyses must be performed and appropriate measures taken in order to ensure that the response times are improved. If the response time is not met in two consecutive months, this counts as non-compliance with the SLA.

The response times from SAP development, the SAP consolidation system and the SAP JAVA system, as well as from non-SAP systems, must correspond at least to today’s standard, and may not impair the SAP functionality for the users.

B.4 Deadlines for Batch Processing

Provided that no job terminations or similar occur, the following time frames and deadlines have to be kept to for batch processing:

PE1, PG1, PA1, PP1, PM1	Night batch chain completed by 7:00 local time PE1,
PG1, PA1, PP1, PM1	Daily backup completed by 23:30 local time PE1,
PG1, PA1, PP1, PM1	BW trigger event completed by 06:00 local time
PW1	Data transfer from ERP systems by 8:00

During the transition phase, additional deadlines are added if required

B.5 Error Handling and Troubleshooting

The following incident remedy times apply:

Incident priority 0 (auto-reaction)	1-10 min (depending on automation)
Incident priority 1 (critical) incident	2 hrs
Priority 2 (major)	8 hrs
Incident priority 3 (standard)	24 hrs
Incident priority 4 (request)	48 hrs

For critical business processes, the error priority classifications apply. VIP support must be guaranteed (such as Yellow Book in BW for senior management, HR for senior management, incidents at VIPs).

For the auto-reactions already defined using automation processes in the existing Customer Standard, priority 0 applies (for example file system monitoring, database restart upon termination, automatic reaction to hardware outages, and automatic SAP data pool enlargement when 95% of the maximum level is reached). The automatisms are necessary in order to ensure that SAP runs 24 x 7.

During the transitional phase, the escalation scenarios are defined.

Legal Notice

We expressly point out that this document cannot anticipate and cover all regulatory requirements of all DSAG members in all business scenarios. There is therefore no claim to completeness with regard to the issues and suggestions discussed. The DSAG and participating authors cannot assume any responsibility for the completeness and suitability of the suggestions.

Deutschsprachige SAP® Anwendergruppe e.V.
Altrottstraße 34 a
69190 Walldorf | Germany
Telephone +49 6227 35809-58
Fax +49 6227 35809-59
e-mail info@dsag.de

dsag.de