Leitfaden

Hybrider Betrieb

Betriebskonzepte für SAP-Lösungen.

Autoren

Name	Vorname	Firma	Mail-Adresse
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	Universität Magdeburg	ronny.zimmermann@ucc.ovgu.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

THEMENGEBIETE

1 Einleitung/Modellunternehmen

Viele Unternehmen stehen vor der Herausforderung, ihre bestehenden On-Premise-Landschaften um neue Cloud-Technologien zu erweitern. Der vorliegende Leitfaden soll eine Hilfestellung sein für IT-Basis-Mitarbeiter, die den Weg eines Unternehmens in eine solche hybride Systemlandschaft betreuen. Er basiert auf Best Practices aus unterschiedlichen Unternehmen, die im Rahmen des DSAG-Projekts „Betrieb von hybriden Landschaften“ seit 2017 zusammengetragen wurden. Hierbei handelt es sich um das Nachfolgeprojekt von „Die SAP-Basis von morgen“, das sich bereits mit den zukünftigen Anforderungen an eine IT-Basis-Abteilung beschäftigt hatte.

Vorweg kann gesagt werden, dass es deshalb nicht *eine* richtige Herangehensweise oder *einen* idealen Aufbau *einer* hybriden Landschaft gibt, da sich die IT-Landschaft jedes Unternehmens auf Basis von vergangenen Entscheidungen und Geschäftstätigkeiten vom Aufbau her unterscheidet. Jedoch möchten wir auf potenzielle Problemstellungen und Themen aufmerksam machen, die es generell beim Betrieb hybrider Landschaften zu beachten gilt, jeweils mit Referenz auf die von SAP bereitgestellten Tools.

Joe‘s Fidget Spinners AG – Das Modellunternehmen für den hybriden Betrieb

Eine hybride Landschaft besteht also aus verschiedenen Cloud-Lösungen (IaaS, PaaS, SaaS) und On-Premise-Systemen. Um die Funktionsweise dieser Systemlandschaft zu verdeutlichen, soll als Beispiel für ein Unternehmen mit einer solchen hybriden Landschaft der Hersteller von Trend-Spielzeug Joe’s Fidget Spinners AG dienen:

Das Unternehmen Joe’s Fidget Spinners AG agiert seit Jahren erfolgreich am Markt. Rasantes Wachstum und neue Technologien erforderten bald Veränderungen des Geschäftsmodells und damit die Transformation der IT.

- Das Business möchte den Vertrieb, bisher ausschließlich über Vertreter abgebildet, um einen weltweiten Endkunden-Direktvertrieb mittels Web-Shop ergänzen. Dabei soll es dem Kunden auch möglich sein, Individualisierungen an den Produkten vornehmen zu können (Losgröße 1) und sich über den Status seiner Bestellung zu informieren. Infolgedessen wurde aufgrund von Sicherheitsaspekten und der weltweiten Verfügbarkeit entschieden, die dafür nötigen Services nicht im eigenen Data Center aufzubauen, sondern eine Platform-as-a-Service-Lösung in der Cloud zu nutzen.

- Diverse Fachbereiche sind unzufrieden mit der Umsetzungsgeschwindigkeit von IT-Projekten, vor allem wenn Services nicht nur intern, sondern auch nach außen zur Verfügung gestellt werden sollen. Um die Stabilität der Kernsysteme (Digital Core) weiterhin zu garantieren und gleichzeitig eine höhere Entwicklungsgeschwindigkeit bei nicht kritischen bzw. agilen Systemen zu ermöglichen, werden bestimmte Entwicklungen und Erweiterungen nicht mehr auf internen Systemen programmiert, sondern Unternehmen nutzen *Platform-as-a-Service*-Angebote als Entwicklungs- und Laufzeitumgebung.
- Die IT will ihre internen Hard- und Software-Ressourcen besser auslasten und Peaks aus Projektsituationen nicht mehr in Capex (Investitionsausgaben), sondern in Opex (Betriebskosten) abgebildet sehen. Daher sollen die Ressourcen für Systeme, die nur temporär genutzt werden, bei einem *Infrastructure-as-a-Service*-Anbieter nur für den Nutzungszeitraum angemietet werden.

Joe‘s Fidget Spinners AG arbeitet seit langer Zeit mit SAP als zentralem ERP-System und verfügt daher in ihrer IT-Organisation über entsprechend umfangreiches Know-how. Als langjähriges Mitglied der DSAG waren und sind die Kollegen immer up to date, was die aktuellen Trends und Entwicklungen rund um SAP betrifft. Ein wichtiger Impuls für die SAP-Basis der Joe‘s Fidget Spinners AG und deren Organisation war der DSAG-Leitfaden „SAP-Basis von morgen“. Nach gründlicher Analyse der eigenen Situation haben die Verantwortlichen der Joe‘s Fidget Spinners AG erkannt, dass bei dem Weg in die hybride Welt der Betrieb nicht schlanker, sondern komplexer wird.

Heute ist die Systemlandschaft der Joe‘s Fidget Spinners AG eine hybride Landschaft, bestehend aus den folgenden Systemen und Anwendungen, welche entweder im eigenen Rechenzentrum betrieben werden oder von SAP als Cloud-Lösung oder Plattform bereitgestellt werden.

Die On-Premise-Systeme der Joe‘s Fidget Spinners AG:

- SAP S/4HANA – der Digitale Core für die betriebswirtschaftlichen Kernprozesse verbleibt entsprechend der Unternehmensstrategie im Haus.
- SAP BW – die Analyseumgebung wird aus dem zentralen System versorgt und stellt das komplette Reporting für das Unternehmen bereit.
- SAP PO – da das Unternehmen eine Reihe unterschiedlicher Schnittstellen bedienen muss, wird das SAP-PO-System konsequent als zentrale „Datendrehscheibe“ genutzt. Dies gilt auch für den Datenaustausch mit Anwendungen und Diensten, die aus der Cloud bezogen werden.
- SAP Solution Manager – Dieser ist zentrales Werkzeug für die Verwaltung der SAP-Systemlandschaft, technisch (Monitoring, Service Desk usw.) und auf Applikationsebene (Solution Dokumentation, Test Management usw.).

- SAP Landscape Management (SAP LaMa) – der Landscape Manager dient der SAP-Basis zur technischen Steuerung der Systemlandschaft und übernimmt wichtige Funktionen, wie z. B. Systemkopien.
- MES (non-SAP) – zum Anschluss der eigenen Produktion bzw. des Produktionssystems an das zentrale ERP dient ein Manufacturing-Execution-System.
- SAP Cloud Connector – dieser bildet die technische Komponente zur Verbindung von On-Premise-Systemen mit SAP Cloud Platform.

Die Cloud-Anwendungen und Plattformen der Joe‘s Fidget Spinners AG:

- SAP Cloud Platform – der Webshop für den weltweiten Direktvertrieb ist als Anwendung auf der SAP Cloud Platform programmiert.
- SAP Cloud Platform Integration Service – als Gegenstelle zur On-Premise-Datendrehscheibe PO verbindet er die On-Premise-Systeme mit den Cloud-Anwendungen.
- Cloud for Customers – alle Vertriebsprozesse für die Vertreter werden über diese SaaS-Lösung abgebildet.
- IaaS Public Cloud – die Firma nutzt in Projekten für Sandbox, PoCs und Trainingssysteme die Ressourcen eines IaaS-Anbieter zur temporären Bereitstellung von Systemen.

Im Folgenden ist die Systemlandschaft graphisch dargestellt:

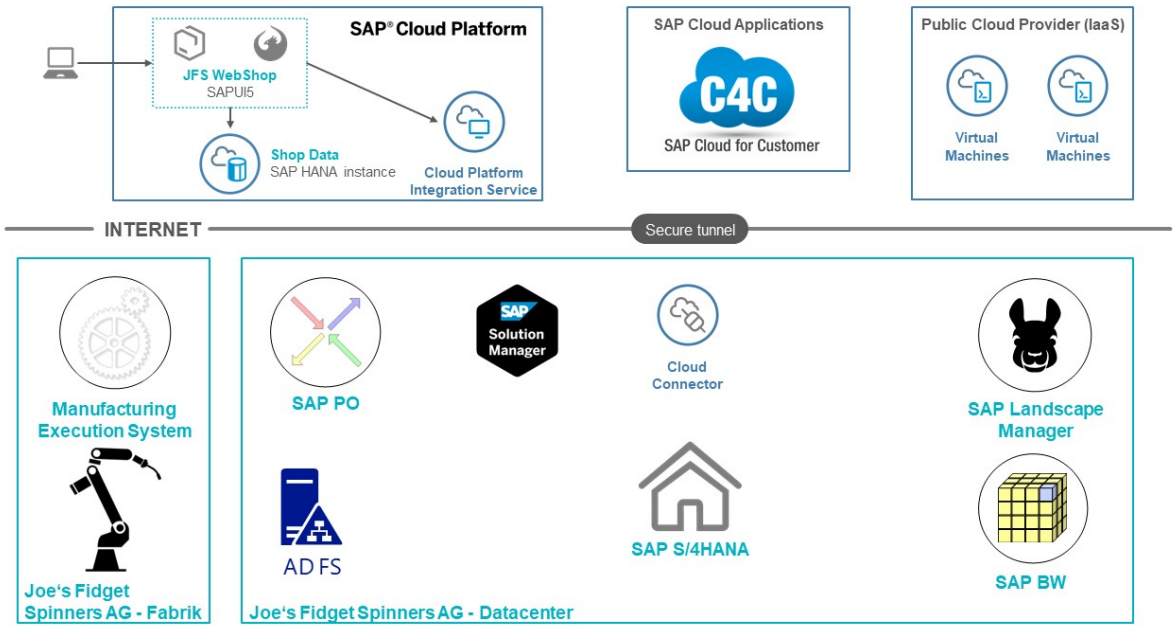

Abbildung 1: Cloud-Anwendungen und Plattformen der Joe‘s Fidget Spinners AG

2 Begriffsklärung

Wir unterscheiden zwischen den folgenden Landschaftsarten[1]:

- On-Premise-Landschaft: kein Einsatz von Cloud-Lösungen
- Hybride Cloud: keine Verwendung von On-Premise-Systemen; verschiedene Cloud-Deployment-Modelle werden genutzt (IaaS, PaaS, SaaS)
- Hybride Landschaft: Verwendung von On-Premise-Systemen und Cloud-Lösungen

Deployment-Modelle und Beispiele:

- On-Premise: Beim Kunden installierte Software, z. B. SAP ERP
- Private Cloud: Software, die vom Kunden in seiner Cloud-Infrastruktur betrieben wird
- Managed Private Cloud: Software/Systeme in der Cloud, die dem Kunden direkt zugeordnet sind (z. B. SAP HANA Enterprise Cloud).
- Infrastructure-as-a-Service (IaaS) Cloud: Cloud-Infrastruktur eines Drittanbieters, die gemietet wird und auf der eigenen Software installiert und betrieben werden kann (z. B. AWS)
- Platform-as-a-Service (PaaS) Cloud: Laufzeit- und Entwicklungsumgebung inkl. zusätzlicher Services, auf der Kunden eigene Software entwickeln und betreiben (z. B. SAP Cloud Platform)
- Software-as-a-Service (SaaS) Cloud: Software wird durch einen Drittanbieter angeboten und betrieben, zur Nutzung durch den Kunden (z. B. SAP SuccessFactors).

3 Discovery & Cloud On-/Offboarding

Dieses Kapitel soll als Checkliste beim Cloud-Onboarding dienen. Zunächst empfehlen wir den Aufbau eines Cloud-Onboarding-Teams, das sich schon ab dem Beschaffungsprozess gemeinsam den Fragestellungen widmet, um Abhängigkeiten frühzeitig zu erkennen. Zudem stellen wir eine technische Checkliste für das Onboarding-Team zur Verfügung.

3.1 Cloud-Onboarding-Team

- Basis-Mitarbeiter: Für die technischen Details, das technische Assessment, Servicekatalog, ITSM, etc. Wir empfehlen, die aktuelle Landschaft zu skizzieren.

[1] Eine gute Übersicht über die verschiedenen Deployment-Modelle und SAP-Offerings findet sich unter https://support.sap.com/en/tools/software-logistics-tools/landscape-management-process.html#panel-section-accordion-accordionitem-body.

- Infrastruktur-Mitarbeiter: z. B. IDM, Netzwerk etc.
- Governance/Security-Mitarbeiter: Zur Klärung von Datenschutzdetails, Ausstiegsklauseln und Sicherheitsdetails
- Fachabteilung: Werden die Business-Anforderungen der Anwender durch die neue Software erfüllt?
- Einkauf: Setzt nicht nur die Konditionen für die erste Nutzung, sondern auch für einen eventuellen Nachkauf für weitere User fest. Offboarding-Konditionen können gegebenenfalls verhandelt werden.
- Entwickler: Sie können Detailfragen zum Erweiterungskonzept der potenziellen Lösung stellen. Kann die Lösung firmenspezifisch konfiguriert werden?

Bei einer Software-as-a-Service-Lösung kann meist die Infrastrukturebene vom Kunden nicht beeinflusst werden und ist daher zu vernachlässigen. Jedoch wird empfohlen, sich die Wartungsprozesse erläutern zu lassen. Bei Wartungsprozessen durch den Anbieter (z. B. Updates) kann die Anwenderlösung verändert reagieren. Bei der Festlegung der Testszenarien sollte darauf geachtet werden. Die technischen Kollegen (Basis) sollten außerdem den kompletten Prozess vom Problem beim Endbenutzer über die Ticketerstellung bis zur Weiterleitung und Lösung durch den Cloud-Anbieter prüfen und testen. Vor allem bei Outsourcing solcher Basis-Tätigkeiten geht intern das Know-how für die technischen Details verloren. Dann muss sogar unter Umständen ein externer Dienstleister für das technische Assessment beauftragt werden.

Insbesondere sollten die Verantwortlichkeiten beachtet und das Hochverfügbarkeitskonzept sowie der Service-Vertrag bei SAP geprüft werden. Die Support-Modelle müssen gegenüber dem bestehenden On-Premise-Vertrag angepasst werden, da die Cloud-Lösungen nicht automatisch mit dem bestehenden On-Premise-Vertrag gekoppelt sind. Leistungen, die bisher abgedeckt sind, sind unter Umständen für die Cloud separat zu buchen.[2]

3.2 Technische Checkliste

3.2.1 Service Level Agreements

Das Service Level Agreement (SLA) ist abhängig von der Lösung und dem Geschäftsmodell des Unternehmens zu erstellen. Wir empfehlen dringend eine enge Abstimmung zwischen dem Fachbereich und der IT, denn es sollten Inhouse Operational Level Agreements wie z. B. Infrastructure Services berücksichtig werden.

Es ist unbedingt erforderlich, dass die Zuständigkeiten des Liefermodells eindeutig in einem gemeinsam abgestimmten *Service-Katalog* festgelegt werden. In den

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

Verträgen bzw. Statements of Work werden in der Regel die Grundprinzipien vereinbart. Hier darf eine präzise Abstimmung der notwendigen Operations- und Maintenance-Prozesse nicht fehlen, die als Grundlage für die praktische Arbeit dienen kann und Verzögerungen im späteren Betrieb vorbeugt.

In den Service Level Agreements sollten auch die Rahmenbedingungen in Form von Service Parametern festgelegt werden. Häufig werden SLAs auf reine Verfügbarkeits-SLAs reduziert, was allerdings unzureichend zur Bewertung der Servicequalität ist. Wir empfehlen eine genaue Festlegung des Messalgorithmus für die Parameter. Es kann beispielsweise hilfreich sein, wenn man spezifische Response Time SLAs vereinbart, abhängig von Prozessen (z. B. SAP Batch, Online, RFC) oder auch E2E SLAs in unterschiedlichen Regionen. Ein Überblick über die Service-Parameter wird imBasisbetrieb SAP (Basisbetrieb) gegeben.

3.2.2 Security Assessment & Data Ownership

Bei der Einführung von Software sollte generell ein Security Assessment durchgeführt werden, um von Grund auf sichere Landschaften aufzubauen (Security by Design). So muss der Zertifizierungsstatus der Cloud-Lösung, aller Integrationskomponenten, auch im Hinblick auf SOC2-Reports überprüft werden. Bei Sonderanforderungen (z. B. Medizintechnikbereich, Automobil etc.) müssen die firmeninternen Compliance-Anforderungen geprüft werden (siehe Security).

3.2.3 Datenschutz der Lösung prüfen

Es muss außerdem geprüft werden, ob alle legalen Voraussetzungen (wo werden die Daten gespeichert, wer kann sie einsehen; Privacy-Shield-Abkommen etc.) erfüllt werden. Hier gilt es zu beachten, dass eine **juristische Prüfung schnell mehrere Wochen dauern kann.**

3.2.4 Datenmigration/-sync/-integration

Die Migration der Stamm-/Bewegungsdaten ist ein Kernbereich im Onboarding-Prozess. Daher sollte der Austausch der Daten, die anzuwendende Technologie wie auch das Mapping frühzeitig geklärt werden. Insbesondere das Mapping der Datenstrukturen kann sehr zeitaufwändig sein. Außerdem müssen legale Anforderungen beachtet werden: In manchen Ländern gibt es besondere Regelungen, wie Daten gespeichert werden müssen (USA/DE, RUS/DE z. B.). Hier ist die Governance-Abteilung gefragt (siehe Integration).

3.2.5 User Management

Eine neue Cloud-Lösung ist sehr wahrscheinlich nicht mit dem bestehenden User Management der On-Premise-Systeme kompatibel. Daher müssen die folgenden Fragestellungen in Zusammenarbeit mit dem Fachbereich und der Governance-Abteilung geklärt werden:

- Wer ist Administrator?
- Wie werden Rechte in der neuen Lösung erteilt?
- Gibt es eine Anbindung an das bestehende IDM?
- Wie wird das Access Management geregelt?
- Wer und wie wird die Provisionierung der Authorizations gemacht?
- Gibt es vorhandene Namenskonzepte, die um Cloud-Themen erweitert werden müssen, z. B. alle Cloud-Benutzer fangen mit einem festen Prefix an und werden durchnummeriert.
- Ist eine Deprovisionierung berücksichtigt worden?

3.2.6 Integrationfähigkeit prüfen

Stammdaten, Bewegungsdaten, SSO, SAML, IDM, Ticket-Anbindung, etc. müssen bei der Integration bedacht werden. Auffällig ist, dass bei der Einführung einer Cloud-Lösung oft der Vertrieb und die Line of Business zu wenig auf das technische Setup achten und die Anbindung der Cloud-Lösung meist unterschätzen. Die interne IT gerät hier schnell in die Verteidigungsposition, da der Cloud-Vertrieb den Integrationsaufwand zu gering geschätzt hat, um den Deal schnell abschließen zu können. Nur die eigene IT kennt die Voraussetzungen und die Governance-Regelungen (Legal) im eigenen Unternehmen. Daher ist es unabdingbar, dass die SAP-Basis in den Auswahlprozess mit eingebunden wird.

3.2.7 Architektur

Alle Schnittstellen zwischen der vorhandenen On-Premise-Landschaft und den neuen Cloud-Lösungen müssen sauber beschrieben werden, als Vorbereitung der Integration in den regulären Betrieb.

3.2.8 Infrastruktur und Monitoring anpassen

Die Netzwerkkomplexität sollte geprüft und die Ports beachtet werden. Die Netzwerkintegration kann sehr aufwändig (Hybris Commerce Suite) sein. Auch müssen Bottlenecks berücksichtigt werden. Darunter fällt auch die Prüfung des globalen Services: Bei lokalen Komponenten muss geprüft werden, ob die lokalen Komponenten die Anforderungen auch global leisten. Das Monitoring enthält hierzu nähere Details.

3.2.9 Netzwerk/Bandbreite

Wo wird die Cloud-Lösung betrieben (Latenzzeit beachten)?
Welche Anforderungen an die Anbindung werden seitens der Cloud-Lösung gefordert? Muss hier etwas Besonderes beachtet werden?
Muss die Bandbreite beim eigenen Internet-Anbieter erhöht werden (Stichpunkt Geocaching)?

3.2.10 Übergabe in den Betrieb

Um einen reibungslosen Betrieb der Cloud-Lösung gewährleisten zu können, muss der zuständige Bereich (Hotline, 1st Level, 2nd Level) informiert und am besten bei der Dokumentation mit eingebunden werden. Bestehende ITSM-Prozesse können dabei helfen, die Struktur der Dokumentation vorzugeben. Zielsetzung ist hier, die neue Lösung und die damit verbundenen IT-Service-Management-Prozesse sowohl graphisch als auch inhaltlich darzustellen, damit im Problemfall zügig die zuständigen bzw. betroffenen Bereiche identifiziert und informiert werden können. Daher empfehlen wir, schon während der Design-Phase die Verantwortlichkeit für die Übergabe in den Betrieb zu klären.

Es gilt zu beachten, dass Monitoring-Schichten der einzelnen Lösungen unterschiedlich arbeiten, z. B. erwarten IaaS-Lösungen normalerweise standardisierte Meldungen. Es muss der Gesamtblick auf das Monitoring für die Firma ins Auge gefasst werden (siehe Monitoring).

3.2.11 Erweiterbarkeit

Ein Vorteil einer Cloud-Lösung ist die Möglichkeit einer einfachen, nachträglichen Kapazitätsaufstockung. Hier sollten der Prozess und der genaue Ablauf (Zuständigkeiten) geprüft werden, damit es bei der Erweiterung nicht zu Überraschungen kommt. Wie sieht die Beauftragung aus (onDemand oder muss jede Erhöhung separat verhandelt werden)? Durch ein geschicktes Anpassen der Verfügbarkeitszeiten an die Betriebszeiten (z. B. Abschalten am Wochenende) können Kosten eingespart werden.

3.2.12 SAP Landscape Governance/Roadmaps

Zum einen empfehlen wir, die allgemeinen *SAP-Landschaftsempfehlungen* zu berücksichtigen:
https://wiki.scn.sap.com/wiki/display/SLGB/Landscape+Recommendations.

Zum anderen sollte auf jeden Fall auch die *Roadmap* der entsprechenden Lösung beachtet werden. Gerade bei Roll-Out-Aktivitäten kann hier gegebenfalls viel Geld gespart werden. Bei den aktuellen Integrationsplänen von SAP sind Synergien sehr wahrscheinlich.

Leitfragen sollten sein:

- Gibt es ein Transportwesen zwischen den Landschaften?
- Wie sieht eine Ideal-Landschaft aus (Landschaftsarchitektur 3-stufig oder 2-stufig)?

Außerdem muss der Release-Zyklus der Cloud-Lösung (z. B. 4-wöchig) zum Unternehmen passen. Wenn die Lösung validiert werden muss (z. B. Medizintechnik), kann sie unter Umständen nicht eingesetzt werden.

3.2.13 Personal: Training

Die Schulung der Mitarbeiter, die mit der neuen Cloud-Lösung zu tun haben, ist unablässig und sollte frühzeitig eingeplant werden. Die Projektlaufzeit kann damit maßgeblich reduziert werden.

Leitfragen sollten sein:

- Wer ist technischer Owner der neuen Lösung?
- Wer kann Services beim Cloud-Anbieter buchen?
- Wie sieht das Rollenkonzept aus?
- Wer kann einen Tenant freigeben?
- Wer ist System-Owner?
- Wer ist Sys-Admin und welche Berechtigungen hat er?
- Wer ist für was verantwortlich?

Beachte: **Verantwortlichkeitsmatrix – Wer macht was?**
Verantwortlichkeiten müssen klar definiert werden.

Alle relevanten Mitarbeiter sollten für die Auswirkungen einer Cloud-Lösung (IaaS, SaaS) sensibilisiert werden. Bei vielen Cloud-Lösungen hängt das Pricing und das Abrechnungsmodell mit der Betriebszeit zusammen. Gegebenenfalls können Systeme am Wochenende oder zu gewissen Zeiten heruntergefahren werden, wenn sie nicht benötigt werden, um Kosten einzusparen. Da solche Themen in der On-Premise-Welt eher unbekannt sind, ist eine Sensibilisierung der Mitarbeiter sinnvoll.

3.3 Wechsel des Cloud-Anbieters/Offboarding

Es kann vorkommen, dass der Cloud-Anbieter gewechselt werden soll. Hierdurch entstehen zusätzliche Kosten. Die Projektphasen (siehe Cloud-Onboarding-Team) müssen wieder abgearbeitet werden. Synergien können im Bereich der Bestandsaufnahme (Anforderungen an die Cloud-Lösungen) bestehen. Oft ist die Migration der Daten zum Cloud-Anbieter kostenfrei. Der Export der Daten zu einem anderen Provider wird hingegen bepreist, um den Cloud-Kunden möglichst lange zu binden.

Beim Offboarding soll die Nutzung der Cloud-Lösung eingestellt werden. Hierbei ist zu klären, welche Aufbewahrungsfristen gelten und wo die Daten künftig verbleiben. Gegebenenfalls nach Rücksprache mit der Governance/Revision-Abteilung ist zu prüfen, ob die Daten in ein firmeneigenes Archiv oder beim Cloud-Anbieter zu Recherchezwecken verbleiben sollen.

Wir empfehlen, die Abhängigkeiten eines Offboardings/Wechsel des Anbieters bereits beim Einführungsprojekt komplett zu durchdenken, um spätere Überraschungen oder erhöhte Kosten zu vermeiden. Schon bei der Auswahl und der Preisverhandlung sollte dieser Punkt berücksichtigt werden.

4 Security

Dieses Kapitel befasst sich mit grundlegenden Überlegungen zu Security-Themen, die bei der Einführung und dem Einsatz von hybriden Landschaften zu beachten sind. Die im Kapitel Cloud-Onboarding-Team angesprochenen Punkte wie Security Assessment, Data Ownership oder Wechsel des Cloud-Anbieters/Offboarding sollen hier vertieft werden. Außerdem bietet dieses Kapitel Hinweise auf versteckte Kosten im Bereich Security Operation und Management.

Das Ziel der Informationssicherheit ist der angemessene Schutz aller Informationen im Unternehmen. Sicherheitsrisiken leiten sich aus dem Risikomanagement ab und sollten anhand der Eintrittswahrscheinlichkeit und des Schadensausmaßes bewertet werden. Mögliche Handlungsoptionen sollten nach ihren Kosten und Nutzen bewertet und den Gefährdungen gegenübergestellt werden. Durch Minimierung der Eintrittswahrscheinlichkeit oder Minimierung des Schadensausmaßes kann das Risiko vermindert werden.

Da sich bei Cloud-Computing, im Gegensatz zum herkömmliches On-Premise-Betrieb, die Governance von Security und Compliance zum Teil auf den Cloud-Provider verlagert, gilt es, vor der Einführung eines Cloud-Services eine entsprechende Risikobewertung durchzuführen, im Zuge derer die Security-Richtlinien, der Umgang mit personenbezogen Daten vor dem Hintergrund der DSGVO sowie der Vereinbarkeit mit den Compliance-Richtlinien des Unternehmens überprüft werden sollten.

4.1 Security Assessment

Ein grundsätzliches organisatorisches Problem beim Cloud-Computing ist, dass für die Provisionierung von Cloud-Services die IT-Abteilung zunächst nicht benötigt wird. Daher werden in der Praxis gerade Cloud-Produkte häufig von der Fachabteilung direkt bezogen. Im Betrieb fällt schließlich auf, dass die Integration von Stamm- und Bewegungsdaten sowie ein zentrales Benutzer-Management benötigt werden.

Ein weiteres Problem bei dieser Praxis ist, dass die Security-Anforderungen an den Cloud-Service nicht überprüft werden, was unter Umständen nicht nur die Sicherheit der eigenen IT kompromittiert, sondern auch rechtliche Schwierigkeiten mit sich bringt.

Aus diesen Gründen empfiehlt es sich, die Security- und Compliance-Abteilungen sowie den Datenschutzbeauftragten von Beginn an einzubinden, um die Landschaft nicht durch eine mangelhafte Integration zu gefährden. Im Idealfall sollte das Security Assessment an erster Stelle stehen.

Zudem reicht es nicht, das Security Assessment nur zur Einführung eines Services durchzuführen, da sich die Services über ihren Lebenszyklus verändern können. Vielmehr sollte ein regelmäßiges Assessment in den Prozessen verankert sein.

Das Assessment selbst und die Implementierung geeigneter Maßnahmen können je nach Umfang einigen zeitlichen Vorlauf benötigen. Zudem können Maßnahmen aus dem Security-Assessment auch vertraglicher Natur sein, was ein Problem darstellt, wenn der Vertrag schon unterzeichnet wurde. Dieser Prozess kann je nach Komplexität bis zu einem Jahr dauern und sollte entsprechend früh eingeplant werden. Im Kontext der SAP Cloud Platform empfiehlt es sich, neben dem Assessment des spezifischen Cloud-Produkts auch SAP als Cloud-Provider selbst und die entsprechenden Rechenzentren zu überprüfen. Da viele SAP-Security-Richtlinien und -Prozesse für mehrere Cloud-Produkte gelten, spart das perspektivisch Zeit bei der Einführung weiterer SAP-Cloud-Produkte. Einzelne Produkte, gerade bei Zukäufen, können sich allerdings auch grundlegend unterscheiden. Es gilt also, den Scope des Assessments zu Anfang genau festzulegen.

Neben dem Assessment des Cloud-Produktes sollten bei einer Integration in die On-Premise-Landschaft auch die Integrationskomponenten, wie Reverse Proxies, Firewalls oder Application Gateways, berücksichtigt werden. Die Cloud-Anbieter betreiben zwar hohen Aufwand, um ihre Rechenzentren gegen Angriffe zu schützen, aber die Sicherheitsmaßnahmen auf Kundenseite müssen ebenfalls bedacht werden. Unternehmen müssen also beim Einsatz von hybriden Umgebungen auch besonderes Augenmerk auf den Schutz der eigenen On-Premise-Systeme legen.

Auf welche Weise ein Assessment durchgeführt wird, obliegt dem entsprechenden Unternehmen. In der Literatur finden sich viele verschiedenene Frameworks und Handlungsempfehlungen. Im Folgenden werden zwei gängige Frameworks und eine Quelle von SAP beschrieben.

4.1.1 CSA Cloud Controls Matrix

Um die Risiken bei Anbietern von Cloud-Computing zu bewerten und geeignete Sicherheitsmaßnahmen zu treffen, bietet die Cloud Controls Matrix (CCM) der gemeinnützigen Organisation Cloud Security Alliance (CSA) ein umfassendes Framework zur Evaluierung sowie Bewertung von Sicherheitsrisiken und den entsprechenden Maßnahmen.

Das Framework umfasst in seiner aktuellen Version eine detaillierte Sammlung von Sicherheitsprinzipien und -konzepten in über 16 Bereichen:

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

Dieses Framework ist Teil einer Sammlung von Standards für Cloud-Computing und beinhaltet die Werkzeuge CloudAudit, das Cloud Trust Protocol und das Consensus Assessments Initiative Questionnaire (CAIQ). Gerade dieser Fragenkatalog zu Sicherheitsfragen bietet Cloud-Kunden einen gute Hilfestellung, um Cloud-Provider zu bewerten und zu benchmarken: https://cloudsecurityalliance.org/star/cloud-customer/.

4.1.2 ENISA Risks of Cloud Computing

Die Studie “Cloud Computing Risk Assessment” der European Union Agency for Network and Information Security (ENISA) beinhaltet eine Risikobewertung zu Cloud-Computing aus Sicht des Cloud-Kunden.

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 on between customer hardening procedures and cloud environment
Legal Risks
Supoena and e-discovery
Risk from changes of jurisdiction
Data protection risks
Licensing risks

Tabelle 1: ENISA Risks of Cloud Computing

Dabei bewertet die ENISA die Security-Risiken nach ihren Eintrittswahrscheinlichkeiten und Auswirkungen und vergleicht Risiken von Cloud-Computing mit denen in einer On-Premise-Landschaft. Zudem klassifiziert die ENISA die Risiken nach politischen, organisatorischen, technischen sowie rechtlichen Risiken.

Die ENISA-Studie gibt einen guten Einblick in Themengebiete, die im Zuge des Security Assessment der Cloud-Lösung zu überprüfen sind. Außerdem werden Best Practices und Security-Maßnahmen zur Reduzierung von Risiken beschrieben.

4.1.3 SAP Cloud Security Framework

Das SAP Cloud Security Framework bietet gerade für SAP-Produkte einen guten Einstieg über Sicherheitskontrollen und -maßnahmen für die verschiedenen SAP-Cloud-Produkte. Das Dokument wird von SAP auf Anfrage herausgegeben und beinhaltet Maßnahmen, Richtlinien und Kontrollen, welche von SAP durchgeführt werden, um Compliance und Sicherheitsstandards einzuhalten. Das Dokument deckt den Großteil der SAP-Cloud-Lösungen ab, jedoch fehlen einzelne Cloud-Produkte. Inhaltlich werden die Themen Informationssicherheit, Datenschutz und Compliance allgemein, und die speziellen Unterscheidungen pro Cloud-Service behandelt. Es gilt herauszustellen, dass dieselben Standards für nicht-produktive wie für produktive Systeme gelten, allerdings nur die produktiven Umgebungen von Auditoren geprüft werden.

4.2 Compliance und Datenschutz

Bei der Einführung von Cloud-Produkten muss sichergestellt werden, dass die rechtlichen Anforderungen und Regularien, die der Kunde zu erfüllen hat, gleichermaßen durch den Cloud-Anbieter erfüllt werden. Neben datenschutzrechtlichen Anforderungen muss der Cloud-Nutzer die geforderten rechtlichen Bestimmungen einhalten (Compliance).

Dies können Anforderungen z. B. aus dem Telekommunikationsgesetz (TKG), der Abgabenordnung (AO) bei der Verarbeitung steuerrechtlicher Daten, dem Handelsgesetzbuch (HGB) bei der Verarbeitung buchführungsrelevanter Daten und dem Strafgesetzbuch (StGB) sein.

Besonders die Übereinstimmung mit den gesetzlichen Vorgaben zum Datenschutz muss bei Cloud-Computing geprüft werden, da nach der Datenschutz-Grundverordnung (DSGVO) der Cloud-Anwender im Außenverhältnis für die Sicherheit der Daten verantwortlich ist. In allen Fällen gilt, dass bei einer Verarbeitung von Daten in der Cloud die Verantwortung in der Regel beim Cloud-Anwender bleibt und dieser sicherstellen muss, dass die Daten beim Cloud-Anbieter gemäß der Vorschriften und Gesetze behandelt werden.

Des Weiteren muss mit dem Cloud-Service-Provider ein Vertrag zur Auftragsverarbeitung geschlossen werden. Neben den allgemeinen Bedingungen der DSGVO ist auf verschiedene Punkte einzugehen. So müssen grundsätzlich alle beauftragten Subunternehmer benannt werden. Wenn weitere Subunternehmer beauftragt werden, muss sich der Cloud-Kunde ein Widerspruchsrecht einräumen lassen, um sich in diesem Fall vom Vertrag lösen zu können.

Ein weiterer Punkt ist die Durchsetzung der Kontrollrechte. Da eine Vor-Ort-Kontrolle oftmals nicht möglich ist, kann das Kontrollrecht auch durch den Nachweis von Zertifikaten erbracht werden. Allerdings ist zu prüfen, ob der konkrete Cloud-Dienst auch in den Anwendungsbereich des Zertifikats fällt. Dies kann oftmals nur durch die Überprüfung der Auditierungsprotokolle gewährleistet werden.

Darüber hinaus muss die Möglichkeit des Anbieterwechsels, des Datenexports, der Datenlöschung nach Auftragsbeendigung und der Verbleib des Eigentums an den Daten beim Unternehmen gewährleistet sein.

4.3 Compliance und Zertifizierungsaudits

Ein gängiges Instrument, um die Einhaltung von Compliance und Sicherheitsstandards zu überprüfen, ist die Auditierung durch unabhängige Prüfgesellschaften. Aus Kundensicht erhöht eine Zertifizierung das Vertrauen in den Cloud-Anbieter. Da die verschiedenen SAP-Lösungen in verschiedenen Rechenzentren und unter unterschiedlichen technischen Voraussetzungen betrieben werden, gilt es, je nach Einsatzgebiet und geografischen Restriktionen sowie regionalen Gesetzgebungen

verschiedene Standards zu prüfen. Im Falle von SAP sind die jeweiligen Cloud-Lösungen nach folgenden Standards zertifiziert:

- 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

Die entsprechenden Zertifikate können im SAP Cloud Trust Center für die entsprechenden Lösungen eingesehen werden. Allerdings muss im Detail geprüft werden, ob die jeweilige Zertifizierung auch für die jeweilige eingesetzte Cloud-Lösung gilt.

Es empfiehlt sich außerdem, die Prüfberichte unter Non-Disclosure-Agreement (NDA) anzufordern und entsprechend der Übereinstimmung mit den kundeneigenen Sicherheitsrichtlinien und Standards zu überprüfen.

4.4 Sicherheitsmaßnahmen

Aus dem Security Assessment der einzusetzenden Lösungen können sich verschiedene Maßnahmen ableiten, um das Risiko hinsichtlich Eintrittswahrscheinlichkeit oder Schadensausmaß zu minimieren. Im Folgenden finden sich einige Maßnahmen und Best Practices, welche aber nicht abschließend sind.

4.4.1 Penetration-Testing

Da in hybriden Landschaften Cloud-Systeme mit On-Premise-Systemen integriert werden, sollten gerade die zentralen Integrationskomponenten abgesichert werden. In den jeweiligen Prüfberichten der Cloud-Lösung wird die regelmäßige Durchführung von Penetration-Tests bescheinigt. Allerdings sollte auch die Infrastruktur des Kunden entsprechend getestet und gehärtet werden. Unter Umständen können daher auch Penetration-Tests der Cloud-Lösung beim Kunden selbst sinnvoll sein. Allerdings gilt es, solche Tests mit dem Anbieter abzusprechen und die Verträge zu prüfen, da sich Penetration Tests, gerade in Public-Cloud-Umgebungen, auch auf andere Kunden auswirken können.

4.4.2 Verschlüsselung & Schnittstellen-Authentifizierung

Grundsätzlich sollte die Kommunikation von Cloud- und On-Premise-Systemen ausschließlich verschlüsselt stattfinden. Dabei gilt es, sichere Verschlüsselungsprotokolle und Technologien einzusetzen und regelmäßig auf ihre aktuelle Version zu überprüfen. Die Verwendung von unsicheren Kryptoalgorithmen und Ciphersuites sollte ausgeschlossen werden.

Für die Authentifizierung der Schnittstellen sollten Zertifikate oder sichere Verfahren wie OAuth2.0 verwendet werden. Auf Basic Authentication über Benutzer und Passwort sollte wenn möglich verzichtet werden. Die regelmäßige Aktualisierung von Zertifikaten erhöht zwar die Sicherheit, in großen verteilten Umgebungen ist der Aufwand allerdings nicht zu vernachlässigen.

Neben der Verschlüsselung des Datenaustausches (Data-in-transfer-Security) über die entsprechenden Schnittstellen sollten auch die Verschlüsselung der Daten in der Cloud (Data-at-rest-Security) gewährleistet und die entsprechenden Schlüssel sicher aufbewahrt werden. Das bezieht sich auf die jeweiligen Tenants, Container oder auch Daten-Backups. Im Security Assessment sollten diese Sicherheitsfragen gezielt überprüft und entsprechende Maßnahmen getroffen werden. Im Idealfall existieren Mechanismen, bei denen der Kunde selbst die Schlüssel festlegen kann. Somit kann das Risiko von unberechtigtem Zugriff durch den Anbieter reduziert werden.

4.4.3 Hardening & Patch Management

Bei der Einführung von Cloud-Services darf man sich nicht ausschließlich auf die Durchführung von Sicherheitsmaßnahmen durch den Anbieter verlassen, da – sobald die Systeme miteinander integriert werden – auch die eigene Infrastruktur gehärtet und entsprechend gewartet werden muss. Gerade die On-Premise-Integrationskomponenten im SAP-Cloud-Umfeld sollten regelmäßig gewartet werden, um Sicherheitslücken zu schließen. Beispielsweise erscheinen für den Cloud Connector regelmäßig kritische Schwachstellen. Diese Sicherheitslücken zu schließen, sollte also fest im Change Management verankert sein, damit eine schnelle Umsetzung möglich ist.

Je nach Betriebsmodell (IaaS, PaaS, SaaS) wird die Infrastruktur, Plattform oder Applikation durch den Anbieter betrieben und gewartet. Das heißt, dass auch abhängig vom Betriebsmodell verschiedene Komponenten durch den Kunden gepatcht werden müssen. So sollte geklärt werden, wer für Fremdbibliotheken verantwortlich ist und wie effizient getestet werden kann. Werden beispielsweise Tools vom Betreiber angeboten, um die Kundenentwicklungen auf Schwachstellen zu überprüfen?

Da beim Design von hybriden Landschaften neue Infrastrukturkomponenten wie Web Application Firewalls, Reverse Proxies oder z. B. der Cloud Connnector aufgebaut werden, erhöhen sich also die Kosten für die Wartung und Weiterentwicklung dieser Komponenten.

4.4.4 Identity Management (IDM)

Bei unberechtigtem Zugriff auf Unternehmensdaten kann großer Schaden für Unternehmen und Kunden entstehen. Im Vergleich zu On-Premise-Anwendungen, welche oft nur aus dem Unternehmensnetzwerk erreichbar sind, ist bei Cloud-Services per se ein Zugriff über das Internet möglich, was das Risiko durch

unberechtigten Zugriff enorm erhöht. Durch die oft enge Integration mit On-Premise-Systemen besteht zudem die Gefahr, dass nicht nur die Daten in der Cloud, sondern auch die On-Premise vorgehaltenen Daten kompromittiert werden.

Damit das Risiko durch Datenmissbrauch reduziert werden kann, sollte gerade in hybriden Landschaften mit verschiedenen Systemen und entsprechenden Berechtigungskonzepten ein zentrales systemübergreifenden Identity Management System (IDM) aufgebaut werden. Zum Beispiel muss sichergestellt werden, dass Benutzer beim Austritt aus dem Unternehmen zeitnah gesperrt werden, da Cloud-Services auch von außerhalb des Unternehmensnetzwerks erreichbar sind.

Entsprechende Prozesse wie die der Benutzeranlage und Sperre sowie die der Berechtigungsvergabe werden im Zuge von Audits und Revisionen nach Standards wie ISO 27000, SOX, BSI oder der EU-DSGVO überprüft.

Ab einer gewissen Unternehmensgröße im mittelständischen Bereich ist zudem der Arbeitsaufwand für die manuelle Benutzerverwaltung und deren Berechtigungen nicht zu unterschätzen und nur noch durch Automatisierung zu begegnen.

Aus diesen Gründen setzen viele Unternehmen bereits im On-Premise-Bereich auf solche IDM-Systeme. Im Kontext von hybriden Landschaften sollte also geprüft werden, wie Benutzer und Berechtigungen in Cloud-Systemen verwaltet werden können.

Ein Standard für die systemübergreifende Verwaltung von Benutzern und Berechtigungen ist das System for Cross-Domain Identity Management (SCIM). Dieses bietet einen einfachen Satz von Befehlen zum Erstellen, Aktualisieren, Lesen und Löschen und basiert auf der Schnittstellentechnologie REST und dem Datenformat JSON. Viele SAP-Cloud-Produkte unterstützen SCIM bereits standardmäßig.

Neben der direkten Anbindung der Cloud-Services an das IDM-System sollte auch die Nutzung des SAP Cloud Platform Identity Provisioning Service geprüft werden. Dieser bietet eine Standardintegration mit den meisten SAP Cloud Platform Services, d.h. das Mapping von Benutzerattributen muss im Idealfall nur an einer Stelle, nämlich zwischen dem On-Premise IDM und SAP Cloud Platform Identity Provisioning, erfolgen. SAP Cloud Platform Identity Provisioning ist insbesondere dann interessant, wenn das Unternehmen für die eigene Benutzerverwaltung kein eigenes IDM betreibt.

Im Hinblick auf die DSGVO gilt es zu prüfen, ob die jeweilige Cloud-Anwendung Mechanismen unterstützt, um Benutzerinformationen bei Bedarf zu löschen.

4.4.5 Access Management (IAM)

Neben der Pflege von Benutzern und Berechtigungen über ein zentrales IDM-System sollte sich außerdem Gedanken über einen zentralen Identity Provider für die Authentifizierung gemacht werden.

Ein sehr verbreiteter Standard für diesen Austausch von Authentifizierungs- und Autorisierungsdaten im Internet ist die Security Assertion Markup Language 2.0 (SAML 2.0).

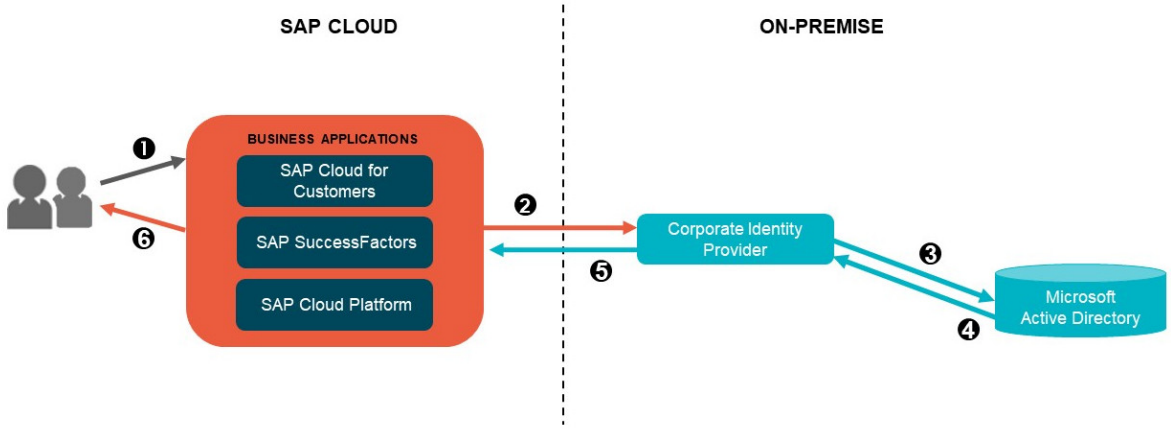

Abbildung 2: SAML-Authentifizierung

In Abbildung 2 ist ein vereinfachter Ablauf beschrieben, bei dem die Authentifizierung an den Corporate Identity Provider delegiert wird. Dieser prüft im Beispiel, ob ein gültiger Active Directory Benutzer existiert und gibt anschließend einen Access Token zurück, über den sich der Benutzer authentifiziert. Ein solches System bietet mehrere Vorteile.

Beispielsweise lässt sich Single Sign-On über Cloud und On-Premise-Systeme hinweg realisieren. So muss der Benutzer, nachdem er sich an seinem Notebook angemeldet hat, beim Aufruf der entsprechenden Cloud-Anwendung keine Zugangsdaten mehr eingeben, sondern die Authentifizierung läuft im Hintergrund über den Identity Provider (IDP).

Außerdem lassen sich am Corporate Identity Provider verschiedene Sicherheitsrichtlinien festlegen, über die beispielsweise gesteuert werden kann, dass sich ein Benutzer außerhalb des Unternehmensnetzwerks über einen zweiten Faktor authentifizieren muss.

Sofern das Unternehmen keinen eigenen Identity Provider betreibt, kann der SAP Cloud Platform Identity Authentication Service (IAS) genutzt werden. Die meisten Cloud-Services bieten eine Standardintegration. Daher kann es auch sinnvoll sein, IAS vor den Corporate Identity Provider zu schalten, um die Anbindung von SAP Cloud Platform Services zu beschleunigen.

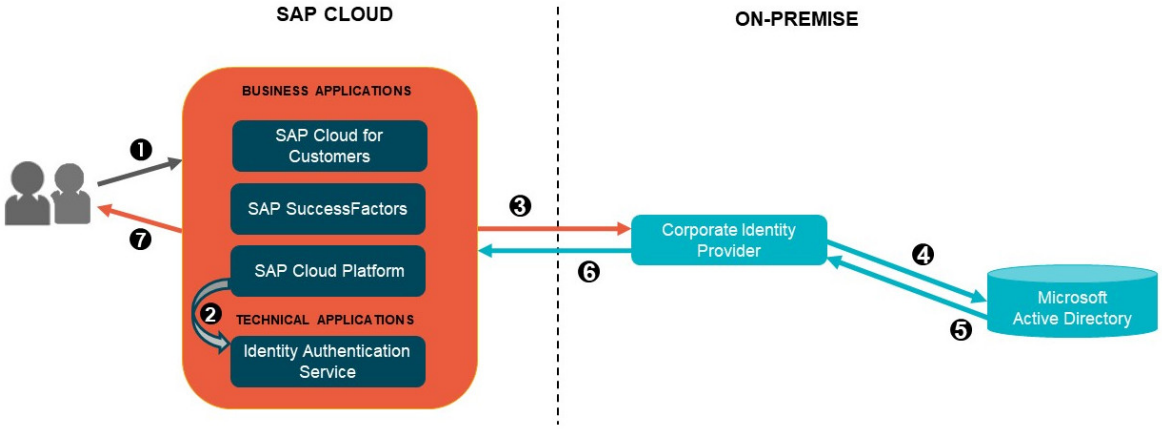

Abbildung 3: SAML Authentifizierung über IAS

In Abbildung 3 ist die Authentifizierung über IAS und den Corporate Identity Provider dargestellt. Weitere Vorteile neben der Standardintegration mit den meisten SAP-Cloud-Diensten sind Funktionen wie die Anbindung unterschiedlicher User Stores für beispielsweise externe Benutzer und Benutzer für den SAP Support, welche dadurch nicht zusammen mit internen Benutzern im Active Directory gepflegt werden müssen oder aufgrund von Sicherheitsrichtlinien nicht gemischt werden dürfen.

Aus Risikosicht ist zu erwähnen, dass ein zentraler Identity Provider eine höchst kritische Komponente in der Landschaft darstellt. Ist diese Komponente nicht verfügbar, kann sich kein Benutzer mehr authentifizieren. Es sollten also geeignete High-Availability-Maßnahmen getroffen werden, um diesem Risiko vorzubeugen.

Um Performance Bottlenecks beim Login vorzubeugen, sollten global agierende Unternehmen ein dezentrales Setup (in verschiedenen Regionen) eruieren.

Hier entstehen unter Umständen nicht geplante Kosten, wenn der zentrale IDP nicht verfügbar ist oder nicht dezentral aufgebaut ist. Auch die Pflege von Authentifizierungsrichtlinien und der allgemeine Betrieb dürfen nicht vernachlässigt werden.

Je nach Lizenzmodell des Identity Providers können hohe Kosten entstehen, wenn beispielsweise nach Login Request abgerechnet wird und die Anzahl der angebundenen Systeme sukzessive steigt.

Im Zuge von mobilen Applikationen für iOS oder Android sollten die Cloud-Services am besten OAuth unterstützen. Bei reiner Authentifizierung über SAML geht ansonsten häufig die Session verloren, wenn der Benutzer die App schließt oder das Betriebssystem die Applikation suspendiert. In der Praxis müssen sich Benutzer also mehrmals am Tag authentifizieren. Über OAuth ist es möglich, die Session über den Neustart der App hinweg vorzuhalten. Die initiale Authentifizierung funktioniert dabei über SAML 2.0 Bearer Assertion Flow for OAuth. Nachdem sich also der Benutzer

über SAML authentifiziert hat, wird der OAuth Token ausgestellt, der je nach Konfiguration für eine Dauer von mehreren Tagen gültig sein kann.

4.4.6 Landschaftsarchitektur & Netzwerksicherheit

Die verschiedenen SAP-Cloud-Lösungen haben verschiedene technologische Unterbauten. Bei der direkten Integration mit Drittsystemen sollten alle Schnittstellen gelistet und daraufhin überprüft werden, ob sie direkt aufgerufen werden können oder eine Middleware benötigt wird. In einer hybriden Landschaft gilt es, genau zu prüfen, ob dedizierte Komponenten wie der Cloud Connector im Falle der SAP Cloud Platform benötigt werden oder ob die Verbindung über andere kundenspezifische Reverse Proxies und Firewalls aufgebaut wird, die vom Anbieter unterstützt werden. Im Idealfall sollte die Verbindung in die SAP Cloud Platform über eine zentrale Komponente erfolgen, um die Wartbarkeit zu erhöhen und keine Hintertüren zu schaffen.

Leider ist in gewachsenen hybriden Landschaften häufig keine einheitliche Architektur erkennbar, was in der Praxis zu versteckten Kosten bei Wartung, Troubleshooting oder der Schließung von Sicherheitslücken führt.

4.4.7 Mobile Device Management (MDM)

Viele Cloud-Lösungen bieten mobile Applikationen. Im Hinblick von Mobile Device Management ist zu überprüfen, ob der Zugriff auf die Cloud-Lösung von Geräten aus möglich ist, die nicht durch die jeweilige MDM-Lösung verwaltet werden. Dies ist beispielweise über den Rollout von Client-Zertifikaten oder mittels Key-Value-Verfahren möglich. Zudem gilt es zu überprüfen, ob die Sicherheitsrichtlinien des Unternehmens beim mobilen Zugriff eingehalten werden können oder zum Beispiel der Zugriff ohne Authentifizierung möglich ist.

4.4.8 Backup & Recovery

Da sich die betrieblichen Aufgaben, wie das regelmäßige Backup der Daten, je nach Betriebsmodell (insbesondere bei PaaS und SaaS) bei Cloud-Computing auf den Anbieter verlagern, hat der Kunde keine direkte Kontrolle mehr über die Durchführung und Aufbewahrung der Datenbank-Backups. Umso wichtiger ist es also, dass diese Aufgabe gewissenhaft durchgeführt wird, um im Notfall die Systeme wiederherstellen zu können.

Die ISO 27001- und die SOC-2-Zertifizierung umfassen auch die Überprüfung der Prozesse zur Durchführung und Aufbewahrung von Daten-Backups. So wird beispielsweise überprüft, wie häufig Backups erstellt werden und wie häufig diese in Backup-Rechenzentren repliziert werden, um bei Ausfall des Rechenzentrums das Risiko des Datenverlusts zu minimieren. In den SLAs wird dem Backup-Prozess entsprechend ein maximaler Zeitraum festgelegt, für den Datenverluste entstehen können.

Ein Risiko in hybriden Landschaften entsteht durch die Integration der On-Premise-Systeme. Dem Umstand folgend, dass Stamm- und Bewegungsdaten mit den On-Premise-Systemen repliziert werden, könnten im Falle eines Datenverlusts auf Seiten der Cloud-Anwendungen Inkonsistenzen zwischen den Systemen entstehen. In einem solchen Fall existiert die Möglichkeit, die On-Premise-Systeme auf den gleichen Stand wiederherzustellen wie die Cloud-Anwendung, was in der Praxis häufig nicht durchzuführen ist, da zum Beispiel dafür das ERP-System zurückgesetzt werden müsste. Eine weitere Möglichkeit ist die erneute Übertragung aller Änderungen. Alle Nachrichten müssen also im Falle eines Datenverlusts wiederholt an das System übertragen werden.

In einer hybriden Landschaft mit unterschiedlichen SLAs ist es extrem aufwändig, ein solches Disaster-Recovery-Konzept (DSR) zu erarbeiten. Zwar versichern Cloud-Anbieter, dass entsprechende DSR-Tests durchgeführt werden. Diese finden aber nur dediziert für Systeme in der eigenen Betriebsverantwortung ohne Beteiligung der Kunden statt, was dazu führt, dass die vom Kunden erarbeiteten Konzepte nicht ausreichend geprüft werden können.

Sofern möglich sollte sowohl vor Einführung als auch in einem regelmäßigen Turnus ein solcher DSR-Test mit Beteiligung aller integrierten Systeme durchgeführt werden, was zu erhöhten Aufwänden im Betrieb führen kann.

5 Integration

Auch wenn im Umfeld von hybriden Systemlandschaften der Betrieb der Cloud-Services (je nach SLA) oft in der Verantwortung des Service-Anbieters liegt, verbleibt die Verantwortung einer geschickten Integration („Ownership“) immer im eigenen Unternehmen.

Die folgenden Abschnitte beschäftigen sich mit der Systemintegration, insbesondere im Hinblick auf die Prozessintegration und die Datenintegration. Im Kontext immer komplexer werdender hybrider Landschaften laufen betriebswirtschaftliche Prozesse (noch) mehr über Systemgrenzen hinweg. „Digitalisierung macht Systemlandschaften komplexer. Geschäftsprozesse enden nicht an einer Applikationsgrenze, sondern sind aus verschiedenen Anwendungen zusammengesetzt oder orchestriert.“[3] Somit kann eine geschickte Systemintegration sogar eine Chance zur Prozessverbesserung sein, insbesondere in deren Qualität und Geschwindigkeit.

Die Systemintegration kann also eine Chance zur Prozessverbesserung sein, insbesondere in deren Qualität und Geschwindigkeit. Somit ist die Systemintegration auch einer der Treiber für Automatisierung – auch in Anbetracht der Industrie 4.0.

[3] Steffen Pietsch auf den DSAG-Technologietagen 2019

5.1 Wann wird Systemintegration relevant?

Systemintegration ist essentiell in hybriden Szenarien und erfordert unbedingt von Beginn an Berücksichtigung. Spätestens bei der Auswahl von Services muss geprüft werden, in welchem Umfang eine Integration in bestehende Szenarien erforderlich ist. Bei der Bereitstellung von Systemen oder Cloud-Services kann es eventuell bereits zu spät sein.

5.2 Was muss bei der Integration von Systemen in hybriden Landschaften berücksichtigt werden?

Im Umfeld der Systemintegration sind zahlreiche Dinge zu berücksichtigen, im Idealfall werden diese bereits während der Auswahl der Systeme und Services geprüft.

Man muss sich zuerst die Frage stellen, ob die Cloud- oder On-Premise-Lösungen die Voraussetzungen der erforderlichen Integration überhaupt erfüllen können. Dies hat direkten Einfluss auf die Aufwände des Implementierungsprojektes und später im Betrieb, beispielsweise bei der Integration in das Monitoring.
Essentiell ist das Vorhandensein von Schnittstellen, die moderne Nachrichtenformate und Transportprotokolle verwenden, um den gewünschten Prozess zu unterstützen. Hier sollte sichergestellt werden, dass die verwendeten Technologien der Schnittstellen zur Integrationsstrategie des Unternehmens passen und die notwendigen Integrations-Tools verfügbar sind. Sollte der Bedarf an zusätzlichen Tools identifiziert werden, können die Aufwände hierfür rechtzeitig Berücksichtigung finden oder sogar zur Wahl anderer Services führen.

Auch sollte geprüft werden, ob (zusätzliche) On-Premise-Systeme notwendig sind, um eine Integration in die bestehende IT-Landschaft herzustellen. Beispielsweise könnten Reverse-Proxies erforderlich sein, die noch On-Premise installiert werden müssen und in die entsprechenden Netzwerksegmente (evtl. DMZ) integriert werden müssen. Werden die On-Premise-Systeme in einer (privaten) Cloud gehostet, können die Partner rechtzeitig involviert werden und der zusätzliche Aufwand hierfür kann entsprechende Berücksichtigung finden.

Das Vorhandensein von vorkonfigurierten Integrationsprozessen („Integration Content“) kann einen großen Vorteil bedeuten. Aufgrund der unterschiedlichen Deployment-Modelle der Cloud-Lösungen (SaaS vs. PaaS) und der vielfältigen Möglichkeiten, wie Integrationen gebaut und verwendet werden, ist dies jedoch im Einzelfall zu betrachten und abzuschätzen. Eine allgemeine Empfehlung kann an dieser Stelle nicht getroffen werden, da Systemintegrationen schlichtweg zu individuell sind. Grundsätzlich ist jedoch empfehlenswert, den ausgelieferten Content genau zu prüfen, um abschätzen zu können, in welchem Umfang dieser für das geplante Szenario verwendet werden kann. Unter Umständen genügt der Content nicht den eigenen Anforderungen und muss erweitert werden – diese Aufwände gilt es, frühzeitig zu identifizieren. Unterschieden wird hier zwischen rein

konfigurierbarem Content, der keine umfassenden Anpassungen erlaubt, und Content, der kopiert und nach Belieben angepasst werden kann. Bei Letzterem geht jedoch aufgrund von individuellen Anpassungen u.U. die Möglichkeit von automatisierten Updates auf neuere Content-Versionen verloren.

Viele Software-Hersteller, darunter auch SAP, verfolgen eine „API first“-Strategie. Hier werden Interface-Bausteine meist als OData- oder Web-Service bereitgestellt, um Systeme damit zu verbinden. Es ist somit empfehlenswert, die API-Repositories der Hersteller (bespielsweise den SAP Business Hub) zu sichten, um dann eine Entscheidung für den Einsatz dieser Technologien zu treffen. Beim extensiven Einsatz von APIs sollte ein entsprechendes Management-Tool, wie z. B. das SAP API Management, in Erwägung gezogen werden. Mit diesen Tools kann Anforderungen in den Bereichen API-Bereitstellung, Security, Traffic Management, Metering und Analytics begegnet werden.

Die Verschlüsselung, Authentifizierung und Autorisierung sollte den selbstgesetzten Anforderungen genügen und zur eigenen Integrationsstrategie passen. Da es hier verschiedene Herangehensweisen gibt, kann nur eine allgemeine Empfehlung ausgesprochen werden. Ebenso sind die Anforderungen der zu integrierenden Services zu berücksichtigen, insbesondere ob die eigenen bisher verwendeten Zertifikate diese erfüllen können.

Besondere Aufmerksamkeit sollte auch den Datenmodellen geschenkt werden. Es gilt herauszufinden, ob die Datenmodelle der zu koppelnden Systeme semantisch zueinander passen, i.e. die Datenkonsistenz sichergestellt sein. Hierfür ist eine frühzeitige Zusammenarbeit mit der Fachabteilung unbedingt anzuraten, um eventuelle Zusatzaufwände abschätzen und einkalkulieren zu können.

Es ist auch zu prüfen, ob die SLAs für die Integration eines Services zu den SLAs, die im eigenen Unternehmen Anwendung finden, passen. Hat beispielsweise ein kritischer Geschäftsprozess eine erforderliche Verfügbarkeit von 99,9%, jedoch werden für die Schnittstellen nur 95% zugesichert, muss damit entsprechend umgegangen werden.

Bei Cloud-Lösungen, insbesondere SaaS, hat die IT des Unternehmens nicht immer einen gleich tiefen Einblick in die Integrationsschicht wie bei bekannten On-Premise-Systemen. Unbeabsichtigte Massenreplikationen sollten dennoch verhindert werden können.

Nicht zuletzt gilt es zu prüfen, ob die Netzwerke die zusätzliche Last, die durch die geplanten Integrationsszenarien verursacht wird, verkraften. Je nach Wichtigkeit der Geschäftsprozesse können zusätzliche Anforderungen umgesetzt werden und z. B. die Ausfallsicherheit durch Redundanz erhöht und die Geschwindigkeit der Datenübertragung verbessert werden (Latenz und Bandbreite).

5.3 Welche Kosten können entstehen?

Integrationskosten unterliegen einer sehr großen Varianz. Es können hier keine konkreten Zahlen genannt werden, vielmehr wollen wir die Kostentreiber benennen, um auf eventuelle versteckte oder unerwartete Kosten aufmerksam zu machen. Generell lässt sich feststellen, dass die Aufwände für die Systemintegration leicht unterschätzt werden. Gerade deshalb gilt auch hier, Transparenz zu schaffen und die Kosten rechtzeitig zu prüfen bzw. abzuschätzen – im Idealfall bereits bei der Auswahl der Systeme und Services.

Lizenzen: Sind die für die gewünschte Integration erforderlichen Komponenten und Services bereits inkludiert, oder werden weitere Lizenzen oder Gebühren anfallen? Geht es hier um einmalige Kosten oder wiederkehrende Kosten, denen evtl. auch ein Mengengerüst zugrunde liegt?

Implementierung: Welche Aufwände entstehen durch die Implementierung? In welchem Umfang sind Anpassungen der Schnittstellen oder des ausgelieferten Contents notwendig? Wie einfach lässt sich ein Service koppeln? Können alle Aufwände intern gestemmt werden oder wird externe Unterstützung durch einen Partner, evtl. durch den Service-Provider selbst, nötig?

Middleware: Steht die erforderliche Middleware (z. B. SAP Process Orchestration oder SAP Cloud Platform Integration) bereits zur Verfügung? Sind die Lizenzen der Middleware ausreichend? Sind die Systemressourcen der Middleware ausreichend oder muss hier erweitert werden?

Zertifikate: Stehen bereits alle erforderlichen (public signed) Zertifikate zur Verfügung? Wie oft müssen diese erneuert werden und welche wiederkehrenden Kosten sind damit verbunden?

Indirekte Nutzung: Fällt die geplante System-Integration unter „indirekte Nutzung“? Hier empfiehlt sich das Gespräch mit dem SAP-Vertriebsbeauftragten.

Infrastruktur-Komponenten: Welche Kosten müssen für zusätzliche Komponenten wie z. B. Reverse-Proxies oder Gateways kalkuliert werden?

Netzwerke: Müssen Netzwerkkomponenten erweitert werden, um bessere Werte bei Latenz und Bandbreite zu erreichen? Sind hier die Verträge mit den Internet-Providern zu ändern? Sind zusätzliche Redundanzen erforderlich, um die gewünschten SLAs zu halten?

Koordination: Gibt es in diesem Integrationsprojekt verteilte Teams, die zusammenarbeiten müssen?

Betrieb: Wie umfangreich werden die Aufwände für das Monitoring sein? Welche regelmäßigen Tätigkeiten fallen im Schnittstellenumfeld an? Wie umfangreich gestaltet sich die Übergabe in den Betrieb?

Skills: Sind die eigenen Mitarbeiter mit den verwendeten Technologien vertraut? Was ist an Know-how aufzubauen? Welches Know-how muss ich durch externe Ressourcen einkaufen?

5.4 Weiterführende Hinweise

Zur Vertiefung der getroffenen Aussagen im Kapitel Integration wird empfohlen:

- SAP Vision for Integrating SAP® Applications in Cloud and Hybrid Environments: CIO Guide
- YouTube-Video der Keynote von Steffen Pietsch auf den DSAG-Technologietagen 2019

6 Betrieb

Die Integration von SAP-Cloud-Lösungen in die vorhanden SAP-On-Premise-Landschaft erfordert initial und für den weiteren Betrieb Aufwände in der SAP-Basis sowie in anderen am Betrieb beteiligten Gruppen.

Abhängig von der Größe der IT-Organisation sollte über virtuelle Teams für Cloud-Lösungen nachgedacht werden. Cloud-Lösungen werden nicht nur im SAP-Umfeld eingesetzt.

Mit der Einführung von Cloud-Lösungen wird die vorhandene Landschaft erst einmal erweitert. Oft werden Cloud-Lösungen aufgebaut, ohne gleichzeitig alte Lösungen konsequent abzubauen. Das Wachstum, das durch Cloud-Lösungen entsteht, muss daher in allen Bereichen des Betriebs berücksichtigt werden.

Wachstum ist nicht nur Masse, sondern auch die Zunahme an Informationen über neue Software und Technologien. In komplexer werdenden Landschaften wächst der Koordinierungsaufwand mit den internen und externen Partnern/Anbietern. Im Fehlerfall steigt der Analyseaufwand erheblich und Verantwortlichkeiten verändern sich.

Im Helpdesk (1. Level) müssen die Mitarbeiter mit neuen Begriffen und Systemen umgehen können. Im „Operating/Application Support“ (2. Level), wo Dinge wie zentrale Überwachung, Jobsteuerung und andere Routine-Aufgaben erledigt werden, muss Verständnis geschaffen werden. Die Abteilungen für die jeweiligen Anwendungen oder die Infrastruktur (3. Level), müssen die neuen Technologien beherrschen, und es muss klar sein, wie die Anbindung auf allen Ebenen funktioniert.

6.1 Organisatorische Voraussetzungen

6.1.1 Beschaffungsprozess/Onboarding

Wie oben im Kapitel Discovery & Cloud On-/Offboarding beschrieben, empfehlen wir schon im Beschaffungsprozess für Cloud-Leistungen über den Einkauf eine Einbindung der IT, da nur diese den Überblick über alle Integrationsaspekte

berücksichtigen kann. Außerdem sollte die Security-/Compliance-Abteilung eingebunden werden. Hier gilt es zu prüfen, ob die Cloud-Lösung den Sicherheitsstandards des Unternehmens genügen.

6.1.2 Incident Management

Abhängig von den Lösungen/Anwendungen müssen Meldungen zu Störungen durch Benutzer (externe Kunden und Mitarbeiter) ermöglicht werden. Die Bearbeitung von SAP-Meldungen (OSS-Meldungen/SAP-Support-Portal) muss in der Basis bleiben, aber es muss eruiert werden, wie die unterschiedlichen Lösungen zur Bearbeitung von Störungen miteinander gekoppelt werden.

Weiterführende Informationen finden Sie im Incident Management.

6.1.3 Problem Management

Hier gelten die gleichen Spielregeln wie bei den bekannten On-Premise-Lösungen. Ähnlich wie beim Incident Management müssen auch die externen Dienstleister eingebunden werden.

Nicht jeder Dienstleister und Provider kann und will in der „Software/Lösung für das Problem Management“ des jeweiligen Kunden arbeiten.

6.1.4 Change Management

Die Auflösung der Abhängigkeiten von Changes wird deutlich komplexer. Auch ist dies abhängig von Umfang und Regelmäßigkeit von Changes in den jeweiligen Cloud-Lösungen. Wir empfehlen daher die Erstellung eines übergreifenden Change- und Relase-Kalenders.

Es muss geklärt werden, wie Changes in die Strukturen und Abläufe integriert werden, ohne dass zusätzliche Downtimes für die Anwendungen entstehen. Vorhandene Definition für die Downtime und SLAs müssen ggf. angepasst werden.

- System-Kopien über die Anwendungsketten hinweg
- Downtimes der Cloud-Lösungen
- Wer bekommt die Informationen, dass es eine Downtime oder gar eine Störung gibt?

Weiterführende Informationen finden Sie im Kapitel 7 Hybrid Lifecycle Management unter Punkt 7.2 Incident Management sowie zu SLAs unter Punkt 3.2 Service Level Agreements.

6.2 Unterschiede der Cloud-Konzepte

Ob nun IaaS, PaaS oder SaaS, diese unterschiedlichen Ansätze habe alle Ihre Vor- und Nachteile und müssen abhängig von den Anforderungen individuell bewertet

werden. Die Unterschiede in den Konzepten hat u.a. das BSI (Bundesamt für Sicherheit in der Informationstechnik) unter Cloud-Computing-Grundlagen beschrieben.

Unter anderem im Expert-Portal von SAP wird unter Public Cloud Operations ein Überblick über diese Verfahren gegeben. Ohne im Detail auf die Unterschiede dieser drei Kategorien einzugehen, stellt sich dennoch die Frage, was bedeutet es für die eigene IT, wenn man das ein oder andere einführen möchte. Welches Ziel verfolgt man?

Es ergeben sich viele Fragen, die es zu klären gilt. Wie muss ich mit Lizenzen umgehen, wenn ich durch IaaS mir die On-Premise-Infrastruktur spare und zum Beispiel nur das Blech in Form von Servern beim Provider einkaufe. Darf ich Software, die ich im Rahmen einer Unternehmenslizenz erworben habe, auch auf Server installieren, die nicht bei mir im Unternehmen stehen? Am Ende spart man sich bei IaaS den Umgang mit dem Blech und einigen Fragen der „physikalischen“ Infrastruktur, alle weiteren Themen verbleiben jedoch im Unternehmen und müssen konsequent weiterverfolgt werden, z. B. Datensicherung oder Monitoring.
Am Beispiel der SAP-Basis ergeben sich für den IaaS-Ansatz praktisch keine Veränderungen im Betrieb.

Bei PaaS hat man vielleicht die Frage der Betriebssystemlizenz geklärt, weil diese bereits Bestandteil der Leistung des Providers ist. Auch werden regelmäßig Backups der Maschinen erstellt. Gleichwohl muss sich jemand mit der Installation der Software beschäftigen und im Fall von Fehlern, diese auch durch Support-Verträge oder externes Know-how weiterverfolgen. Gerade Exoten im Betrieb (wenig Masse) sind prädestiniert, um sie in die Cloud abzugeben.
Am Beispiel der SAP-Basis könnte somit die Datenbank-Administration abgegeben werden, da diese vom PaaS-Dienstleister zur Verfügung gestellt wird.

Will man auch das abgeben, landet man bei SaaS. Die Lösung steht auf Knopfdruck bereit und muss nur noch mit Daten gefüllt werden. Integrationen dieser Lösungen sind weiter nötig und werden auch in der SAP-Basis einen gewissen Aufwand generieren.

Welche dieser drei Varianten man immer auch wählt, am Ende des Tages muss bei allen geprüft werden, ob die ausgehandelten SLAs eingehalten werden. Nur durch konsequentes Überprüfen dieser SLAs können mögliche Vorteil wie Kosteneinsparung sichergestellt werden. Ein Prozess wie Incident Management oder Problem Management ist jedoch weiterhin notwendig für den „Betrieb“.
Sprich: Nicht alle (IT-)Aufgaben lassen sich durch Cloud-Lösungen auslagern.

6.3 Landscape Management – Prozess im SAP Solution Manager

Der Landscape Management Process dient im Kern dazu, Daten der IT-Landschaft über *System Landscape Directory* (SLD) und *Landscape Management Database* zu sammeln und zur Verfügung zu stellen.

Zum einen dienen diese Daten zur Berechnung von Änderungen der Landschaft – wie Update, Upgrade und Conversion –, zum anderen werden diese Daten anderen Funktionen zur Verfügung gestellt – ein prominentes Beipiel ist das Monitoring der IT-Landschaft. Mit der Einführung der Cloud-Lösungen wurde die Möglichkeit geschaffen, eine hybride Landschaft aus Cloud- und On-Premise-Systemen zu betreiben. Grundsätzlich sollten hier die SAP-relevanten Cloud-Systeme soweit möglich in den Solution Manager eingebunden werden. Das ist für ein durchgängiges Monitoring der SAP-Landschaft notwendig.

Die Seite Landscape Management Process auf dem SAP-Support-Portal beschreibt diese Kernfunktionen und erweitert sie um Hintergrundinformationen zu den verschiedenen Deployment-Modellen und das große Bild des Change Managements, das entweder mit dem Maintenance Planner – für selbst verwaltete Systeme des Kunden – erfolgt oder durch Subscription von Cloud-Services.

Ergänzt wird diese Information durch Überblicksinformationen zu

- Integration der Landschaft,
- Entwicklung,
- Transport-Werkzeugen
- und erweiterten Möglichkeiten für den Betrieb mit SAP LaMa.

6.4 Application Operation

Unter anderen sind folgende Aufgaben/Aktivitäten für den Betrieb zu sehen, die auch für Cloud-Lösungen gelten. Einige Tätigkeiten müssen zwangsläufig durch die eigene SAP-Basis erledigt werden.

Die nachfolgenden Punkte dienen als *Checkliste* für Operationen, die durchgeführt werden sollten. Hier muss im Einzelfall geprüft werden, wer die Verantwortung trägt. In einer Public Cloud ist der Cloud Provider für viele dieser Punkte verantwortlich. In einer Private Cloud hängt es vom Service Level Agreement (SLA) ab, auf den man sich geeinigt hat.

Checkliste

- Starten/Stoppen, Wartung
- System Copy, System Refresh
- Monitoring
- Zertifikatsmanagement
- Jobsteuerung
- Testing
- Koordination von System-Downtimes/-Updates/-Patches usw.
  Das ist ein nicht zu unterschätzender und unter Umständen hoher Aufwand.
- Wer erstellt die Dokumentation (Betriebshandbücher) für die Cloud-Lösung auch im Zusammenspiel mit den vorhandenen On-Premise-Lösungen?
- Credit Request/Penalty: Wenn die SLAs gerissen werden, müssen diese in Rechnung gestellt werden?
- Wann wird die Cloud-Lösung an den Betrieb übergeben?
- Welche Voraussetzungen müssen für die Übergabe geschaffen werden?
  - Abstimmung mit den beteiligten Gruppen
  - Bereitstellung eines Betriebshandbuches
- Wo ist die Grenze der Verantwortlichkeit?
- Wer darf OSS-Meldungen erstellen?
- Wie sieht es mit der Erweiterbarkeit/Skalierung der Cloud-Lösung aus?
- Wie geht man mit „validierten Systemen“ um?

6.4.1 Downtimes synchronisieren

Wie kann sichergestellt werden, dass bei geplanten Arbeiten an der Cloud-Lösung diese Informationen z. B. auch im System Monitoring des Solution Manager nutzbar sind?

Geplante Arbeiten in den Cloud-Lösungen müssen im Betrieb bekannt gemacht werden, um diese Informationen mit den On-Premise-Lösungen zusammenbringen zu können. So müssen mögliche Einflüsse für eine Downtime dahingehend berücksichtigt werden, dass eine Schnittstelle auf der On-Premise-Seite während der Downtime nicht zur Verfügung steht. In dieser Zeit sollten dann zum Beispiel für diese Schnittstelle keine Störungen gemeldet werden. Ziel sollte es auch sein, solche Arbeiten zwischen Cloud und On-Premise-Systemen sinnvoll miteinander zu verknüpfen.

6.4.2 Portale für Cloud-Lösungen

Eine große Herausforderung ist die unüberschaubare Anzahl von Portalen. Mit dem Start eines Cloud-Projektes muss geklärt werden:

- Welche URLs stehen zur Verfügung?
- Welcher Benutzerkreis/welche Rollen sind für welches Portal angedacht?
- Welche Produkte sind in welchen Portalen zu finden?
- Welche Aufgabe hat das Portal?
- Wer verwaltet die Berechtigungen?
- Welches sind die relevanten Komponenten, die für das Anlegen von Support Calls genutzt werden sollen?

6.5 Reporting

Die SLA der unterschiedlichen Lösungen müssen überwacht werden, damit Stabilität und Verfügbarkeit sichergestellt werden und gegebenenfalls Ansprüche an den Dienstleister geltend gemacht werden können. So kann durch eine einfache Klickfolge im Browser ein Login auf einer Webseite genutzt werden (im SAP Solution Manager durch User Experience Monitoring – UXMon), um zu überprüfen, ob das System erreichbar ist. Dieser Monitor kann dann abhängig von den festgelegten Schwellwerten einen Alarm auslösen bzw. die Verfügbarkeit der Lösung ermitteln.

Wichtig ist eine Überwachung der SLA vonseiten der Kunden. Eigene Berichte zu diesen SLA können dann monatlich generiert und den Verantwortlichen zur Verfügung gestellt werden. Desweiteren sollten die Berichte der Provider unbedingt kontrolliert werden.

6.6 Monitoring

Für den stabilen Betrieb einer SAP-Landschaft ist eine Überwachung aller angeschlossen Systeme und Komponenten wünschenswert. Elemente wie Systemüberwachung (CPU, Festplatten etc.), Schnittstellen-Monitoring bis hin zur Simulation von einzelnen Klickfolgen der Benutzer und ganzen Business-Prozessen sollten dabei berücksichtigt werden. Auch Reports über die zeitliche Entwicklung von KPIs ermöglichen proaktives Handeln, um Störungen möglichst zu vermeiden.

Es muss ein Abgleich von Changes bzw. Transporten sowie vor allem von Downtimes erfolgen, um Fehlalarme zu vermeiden.

Die unterschiedlichen Cloud-Lösungen bieten zum Teil eigenständige oder auf Open Source basierte Monitoring-Lösungen über unterschiedliche Oberflächen an. Diese stehen dem Kunden nur zum Teil bzw. mit eingeschränkten Berechtigungen zur Verfügung.

In einer hybriden Landschaft muss somit die Überwachung der eigenen Landschaft inkl. aller Cloud-Anwendungen sichergestellt und bestenfalls in bestehende Monitoring-Lösungen integriert werden.

6.6.1 Central Monitoring Cockpit

Im Idealfall existiert ein zentrales Monitoring User Interface, auf dem man auf Anhieb erkennen kann, in welchen Bereichen es Fehler gibt. Außerdem muss es Sichten geben, die in Abhängigkeit von der Rolle (Admin, Helpdesk, Operation…) und den Anwendungen (Sales, Service, Logistic…) eine Information über die jeweiligen Systeme geben. Diese Informationen müssen aus unterschiedlichen Monitoring-Lösungen über Technologiegrenzen hinweg zusammengeführt werden.

Im SAP Support Launchpad existiert ein zentrales Monitoring Cockpit, in welches nach und nach die SAP Cloud Services integriert werden sollen:

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

6.6.2 Technisches Monitoring

In jeder Cloud-Lösung, ob als „Funktionsbaustein“ im Hintergrund arbeitend oder zum Beispiel als Teil des B2C-Shops, wird irgendwann eine Störung aufkommen. Unabhängig von der Ursache wird eine solche Störung über das technische Monitoring (oder durch einen Benutzer) gemeldet. Dabei muss sichergestellt werden, das solche Meldungen richtig zugeordnet werden können. Ziel muss es sein, die Meldung mit einer Priorität zu bewerten, die richtigen Verantwortlichen zu finden und auch die Bearbeitungszeit zu optimieren. Bei Bedarf müssen entsprechende Eskalationen angestoßen werden.

Bei den technischen Meldungen müssen die Meldungstexte eindeutig identifizierbar sein. Im SAP-Umfeld ist z. B. die SID/Mandant ein guter Indikator, um eine Meldung einordnen zu können. Bei der Meldung durch den Benutzer, wird dies schwieriger, wenn sich dieser etwa auf einer Webseite befindet. Wo genau befindet er sich und wie kann hier eine möglichst saubere Identifizierung der Anwendung erfolgen? Natürlich gilt diese Fragestellung auch für On-Premise-Anwendungen – gleichwohl muss auch für eine Cloud-Lösung eine Identifizierung durch die „Hotline“ möglich sein. Dabei ist es völlig egal, ob der Anruf (oder Mail etc.) durch einen externen Kunden/Nutzer erfolgt oder durch einen Kollegen aus dem eigenen Unternehmen.

Grundsätzlich gelten die Anforderungen an die On-Premise-Monitoring-Lösung ebenso für die Cloud-Lösungen. Allerdings muss geklärt werden, welches Monitoring selbst durchgeführt werden muss, da bei Cloud-Lösungen der Betrieb teilweise nicht im eigenen Haus liegt. Grundsätzlich hat IaaS hier einen höheren Aufwand als SaaS oder PaaS.

Exception Management muss durch den Provider erledigt werden, abhängig von der IaaS, SaaS oder PaaS. Das System-Monitoring wie CPU oder Memory-Auslastung

sowie Platten-IO ist unter Umständen ein guter Indikator. Vor allem dann, wenn sich Metriken wie Antwortzeiten erhöhen.

In jedem Fall sollte für Cloud-Lösungen durch Funktionen wie E2EMon/UXMon (User Experience Monitoring) ein Monitoring durchgeführt werden. Abhängig von den unterschiedlichen Funktionen eines Business-Prozesses kann man durch ausgewählte Klickfolgen bei synchronen Lösungen gleich auch den Durchgriff auf On-Premise-Lösungen prüfen.

Auch sollte zumindest ein Test eines Logins auf das System durchgeführt werden. Für die SLA-Analyse muss sichergestellt werden, dass im Fehlerfall die Erreichbarkeit der Lösung über die Internetanbindung für den Agenten nicht Ursache für einen Fehler ist. Abhängig von den jeweiligen Schnittstellen können diese mindestens auf der On-Premise-Seite geprüft werden (siehe Solution Manager – Interface Channel Monitoring).

End-To-End Business Process Monitoring (E2E-BPM) sollte über die hybride Landschaft hinweg erfolgen, da Geschäftsprozesse normalerweise nicht nur in der Cloud laufen. Ziel muss es sein, das ein Application Owner eine Information bekommt, dass und ob ein solcher Prozess gestört ist.

Anforderung an SAP:

- UXMon Scripte bei Standardlösungen sollte SAP gleich mitliefern.

6.6.3 Manuelles Monitoring

Beim manuellen Monitoring werden Transaktionen in unterschiedlichen Zeitintervallen (z. B. täglich, wöchentlich, monatlich) geprüft. Oft werden solche manuellen Tests an externe Dienstleister abgegeben, wodurch die Qualität oftmals nicht sichergestellt werden kann. Daher empfehlen wir, manuelles Monitoring nur in Übergangsphasen zu nutzen.

6.6.4 Alerting und Incident Management

Für ausgewählte Events sollen Alarme an die jeweilige Incident-Management-Lösung weitergeleitet werden. Es muss beachtet werden, dass Alarme, die in der Cloud-Lösung geschlossen werden (automatisch oder manuell), auch in der On-Premise-Monitoring-Lösung geschlossen werden. SAP CP Alert Notification erlaubt die Weitergabe von Availability Alerts an SAP Solution Manager/FRUN.

6.6.5 Kosten fürs Monitoring

Die Aufwände für Monitoring sind abhängig vom Szenario schwer zu kalkulieren. Das auch aus dem Grund, da „Monitoring“ in jedem Unternehmen sehr unterschiedlich durchgeführt wird. In jedem Fall muss hier eine genaue Prüfung erfolgen, inwiefern diese Aufgaben manuell oder automatisch erfolgen sollen. Auch automatisches

Monitoring zu verwalten/pflegen ist abhängig von der Größe der Cloud-Lösung und unter Umständen ein nicht zu unterschätzender Aufwand.

6.7 Kosten/Aufwände

Wir empfehlen eine genaue Untersuchung der zu erwartenden Kosten beim Betrieb hybrider Landschaften. Folgende Fragen sollten gestellt werden:

- Welche zusätzlichen Kosten entstehen einmalig und/oder im laufenden Betrieb?
- Sind die Aufwände in allen Gruppen geklärt und ist genügend Personal und Kapazitäten vorhanden?
- Wie können die ungeplanten Aufwände durch Störungen greifbar gemacht und abgedeckt werden?

Checkliste

- Die Infrastruktur muss im Vorfeld von Cloud-Projekten cloud-ready gemacht werden.
- Paradigmenwechsel bei Schnittstellen. Bei On-Premise ist man eine tiefe Integration zwischen Systemen über ausgefeilte Technologien gewohnt. In der Cloud-Welt spricht SAP von loser Kopplung.
- Übergreifende Change- und Release-Kalender müssen gepflegt werden.
- Wie werden die unterschiedlichen Incident-Lösungen miteinander gekoppelt?
- Sind die SLAs zwischen Cloud und On-Premise aufeinander abgestimmt? Werden diese überwacht?
- Welche URLs für die Verwaltung der Cloud-Lösungen gibt es? Ist SAP mit dem „Trust Center“ schon so weit, dass es eine Harmonisierung gibt und immer die gleichen Kanäle genutzt werden?
- Wo fallen zusätzliche Aufwände (einmalig/permanent) intern an und sind diese eingeplant?
- Für hybride Landschaften gilt es vor allem, die Überwachung der Landschaft inklusive Cloud als Ganzes zu betrachten und im Idealfall in die vorhandene Monitoring-Lösung zu integrieren.
- Manuelles Monitoring sollte nur in der Übergangsphase genutzt werden.

7 Hybrid Lifecycle Management

7.1 Organisatorische Auswirkungen

Für die Support-Organisation ist eine hybride Landschaft eine große Herausforderung. Folgende Themen sind zu klären:

1. Innerhalb des Unternehmens sind die Verantwortlichkeiten für den Cloud-Support sowie die Change-Management-Verantwortung für die unterschiedlichen Cloud-Anwendungen zu klären.
2. Die benötigten Ressourcen müssen bereitgestellt werden, z. B. kann für die SAP-Basis ein separates (virtuelles) Cloud-Team notwendig sein.
3. Das Personal muss entsprechend geschult werden.

Eine Beschreibung der Prozessschritte der Änderungsplanung sowie der involvierten Rollen findet sich auf den SAP-Seiten unter Landscape Management Process.

7.2 Change und Release Management

7.2.1 Allgemeine Anmerkungen

Im Bereich Change und Release Management unterscheiden wir sowohl in der On-Premise-Welt als auch im Cloud-Umfeld zwischen Application Changes und Wartungs- und Infrastructure-Changes.
Im SAP-Umfeld setzen viele Kunden auf SAP-interne Tools wie z. B. SAP Solution Manager oder Transport Management System (TMS), haben aber meistens noch ein übergreifendes ITSM-Tool, in dem alle IT-Changes erfasst und koordiniert werden. In einer hybriden Landschaft fehlt jedoch oft eine Übersicht zur Koordination der Changes On-Premise und in der Cloud.

7.2.2 Release Management versus Agilität

In On-Premise-Landschaften werden häufig Release-Zyklen definiert, um Eigenentwicklungen im Verbund live zu setzen. Dies reduziert Kosten durch definierte Testzeiträume und trägt zur Stabilität bei. Innerhalb der Cloud wird agil entwickelt und neue oder geänderte Funktionalitäten gehen zeitnah live. Die Herausforderung in hybriden Landschaften ist daher, alle Entwicklungen zu klassifizieren und trotz unterschiedlicher Entwicklungszyklen eine stabile Landschaft zu gewährleisten.

7.2.3 Change Management in hybriden Landschaften für Eigenentwicklungen

- Cloud – Cloud: Für den Einsatz innerhalb der Cloud hat SAP das Tool CALM (SAP Cloud ALM) entwickelt. Application-Management-Funktionen für die Cloud werden nach und nach in CALM abgebildet, analog zu den Funktionen des Solution Managers für On-Premise-Systeme. Hierzu gehört auch das Change und Release Management.

Innerhalb der SAP Cloud Platform kann der SAP Cloud Platform Transport Management Service genutzt werden, welcher einen Transport von Entwicklungs- und Anwendungsartefakten von SAP Cloud Platform erlaubt (z. B. Content von SAP Cloud Platform Integration).

- On-Premise – Cloud
  Wenn SAP Solution Manager und das erweiterte Change and Transport System (CTS+), welches z. B. das direkte Anstoßen eines Transports aus dem Web UI von SAP Cloud Platform Integration anbietet, bereits im Einsatz sind, kann dies für hybride Landschaften beibehalten werden. Für einen synchronisierten Transport von hybriden Änderungen ist die Integration in Change Management-Ansätze mit Quality Gate Management und Change Request Management (ChaRM) möglich. SAP bietet dafür das „Close Coupling“ mit CTS+ an. Hiermit kann ohne manuellen Aufwand über Bundles von On-Premise und Cloud-Applikationen transportiert werden. Aktuell arbeitet SAP noch an einem Compliance Issue in diesem Umfeld (was in Kürze gelöst sein soll). In der Zukunft wird Cloud Application Lifecycle Management (CALM) auch die hybriden Szenarien unterstützen.

7.2.4 Change Management der Cloud-IT-Landschaft

- Cloud – Cloud
  Kunden, die ihre Anwendungen über verschiedene Cloud-Anbieter verteilt haben, müssen sich einen Überblick über die geplanten Changes machen und diese in eine übergreifende Planung eintragen, um über die anstehenden Wartungsfenster informieren und eigene Changes entsprechend planen zu können. Eine Integration dazu ist nicht verfügbar. Für die SAP-Cloud-Anwendungen können die Informationen aus dem Cloud Availability Center gelesen werden.
- On-Premise – Cloud
  Eine Sicht über alle Changes in der hybriden Landschaft ist derzeit nicht verfügbar. Je stärker verteilt die Cloud-Anwendungen laufen, desto komplexer wird der Planungsprozess für Changes. Konnte man im On-Premise-Umfeld die Changes noch unabhängig planen – was bei großen Landschaften auch schon eine Herausforderung war –, gibt es für die hybriden Landschaften nun schon vordefinierte Wartungsfenster, die mitberücksichtigt werden müssen. Es ist wichtig, eine einheitliche Übersicht über alle geplanten Wartungen zu bekommen, um die stetig wachsende Komplexität im Change-Prozess noch zu handhaben. Dazu ist es nötig, über APIs an die entsprechenden Informationen zu kommen oder eine Integration in einem Tool bereitzustellen, wie zum Beispiel im Solution Manager oder im Cloud ALM.

Forderungen an SAP im Bereich Change Management

- Ein zentraler IT-Kalender im Launchpad [für On-Premise- und Cloud-Produkte] und Interface zu anderen ISTM Tools
- Harmonisierung der Downtime-Fenster
- Zero Downtime für alle Cloud-Produkte

Versteckte Kosten

- Aufwand bei der Koordination von Changes On-Premise – Cloud
- Nacharbeiten nach erfolgten Patches in der Cloud bei kurzfristiger Ankündigung

7.3 Incident Management

7.3.1 Tools

Die bestehende Landschaft bestimmt die Vorgehensweise beim Einsatz eines Incident Managements für hybride Landschaften. Es ist wichtig, eine Bestandsaufnahme der bestehenden Prozesse zu haben, um eine Entscheidung für ein Incident Management in der hybriden Landschaft zu treffen. Wenn beispielsweise als Incident Management -Tool SAP Solution Manager eingesetzt wird, empfehlen wir, diesen auch für die hybride Landschaft zu nutzen.

- SAP Solution Manager
  SAP Solution Manager bietet die Funktionalität eines ITSM-Tools für On-Premise-Anwendungen und ist mit der vorhandenen SAP Backend Feedback-Funktion für SAP optimal ausgestattet.
- SAP Cloud ALM
  Cloud Application Lifecycle Management in der Cloud soll nach und nach Funktionen, die SAP Solution Manager On-Premise besitzt, in der Cloud abbilden. Kunden sollten sich regelmäßig über den Stand der Entwicklung auf dem Laufenden halten, um zu prüfen, ob und wann ein Umstieg sinnvoll ist und welche Funktionalitäten vorhanden sind.

7.3.2 Integration

Wenn bereits ein ITSM-Tool im Einsatz ist, ist es sinnvoll, dies weiter zu nutzen. Wenn anfangs keine integrative Lösung zur Verfügung steht, sollten Sie entsprechende organisatorische Vorkehrungen treffen. Incidents können in allen Tools auch manuell erstellt werden. Hierzu empfehlen wir, für die Cloud-Applikationen entsprechende Formulare bzw. Abfragen zu erstellen, um die nötigen Informationen bei Anwendern zu erfragen (zum Beispiel die URL der Applikation, in der das Problem stattfindet).

Gleichzeitig ist es unumgänglich, den Service Desk einzubeziehen und eine Liste der bestehenden Cloud-Infrastruktur und der zugehörigen Applikationen zu erstellen. Sobald eine integrative Lösung vorhanden ist, die diese Informationen standardmäßig liefert, sollte umgestellt und eine Weiterleitung an das zentrale ITSM Tool eingerichtet werden.

In welcher Umgebung das zentrale Tool laufen soll, richtet sich – wie unter Punkt Organisatorische Voraussetzungen schon erwähnt – nach der vorhandenen Landschaft. Dies muss allerdings regelmäßig überprüft werden, da sowohl die Anzahl der Cloud- zu On-Premise-Anwendungen als auch die vorhandenen Funktionalitäten Veränderungen unterliegen.

Es gibt bei SAP derzeit keine einheitliche Strategie. Einige Cloud-Produkte haben ein integriertes Incident Management (z. B. C4C).

- Cloud – Cloud
  Bei einer Cloud-zu-Cloud-Integration fällt die erste Wahl eines Incident Management-Tools auf eine Cloud-Lösung
- On-Premise – Cloud
  In dieser Konstellation stehen On-Premise-Tools im Vordergrund und sollten auf die Möglichkeit einer Integration beider Welten untersucht werden.

Forderungen an SAP im Bereich Incident Management

- Einheitliches Incident Management für alle SAP-Cloud-Produkte und zusätzlich APIs für die Anbindung von On-Premise ITSM Tools
- Bereitstellung einer Funktion analog zur Feedback-Funktion On-Premise, mit der alle im Incident benötigten Informationen automatisch bereitgestellt werden

Versteckte Kosten

- Eigenentwicklungen oder Erstellen von manuellen Tickets ist nötig, dies erzeugt Aufwände in der IT
- Manuelle Tickets sind nicht entsprechend qualifiziert (fehlende Informationen, da nicht automatisch erzeugt). Dies führt zu erhöhtem Aufwand bei der Ticket-Bearbeitung

7.4 Test-Management

Automatisiertes Testen ist in vielen Unternehmen im Einsatz, unter anderem für Regressionstests.

- Cloud – Cloud: Derzeit ist ein automatisiertes Test-Management mit der WEB-IDE möglich, es gibt allerdings keine Integration mit On-Premise-Tools.
- On-Premise – Cloud: Derzeit ist kein integratives Tool bekannt, die Tests müssen aufeinander abgestimmt werden. CALM soll in Zukunft diese Funktion abbilden.

7.4.1 Tools

- CALM
  Cloud ALM wird in der Zukunft Testmanagement für Cloud und hybride Landschaften bereitstellen.
- Solution Manager
  On-Premise-Kunden von SAP können den SAP Solution Manager für Test-Management einsetzen.
- WEB-IDE
  Derzeit für Cloud-Anwendungen einsetzbar.

Forderungen an SAP im Bereich Test-Management

- Es muss die Möglichkeit bestehen, nach Updates in der Cloud automatisierte Tests einzuplanen.
- Integration der WEB-IDE oder entsprechenden Tools (CALM) müssen mit On-Premise Test-Tools integrierbar sein.

Versteckte Kosten

- Integrationstests für hybride Szenarien müssen manuell koordiniert werden, was zu erhöhten Kosten führt.

7.4.2 Link-Empfehlungen zum Thema:

- CTS+
- Cloud Availability Center
- CALM

8 People

Der Weg in die hybride Welt ist für die Mitarbeiter der Anwendungsunternehmen eine große Herausforderung. Im Vergleich zu einer reinen On-Premise-IT ändern sich Rollen, Arbeitsabläufe und Kommunikation erheblich und erfordern den Willen zur Veränderung – etwas, was dem Menschen nicht von Natur aus gegeben ist.

Die Erkenntnis, dass die mit dem Management von SAP-Anwendungen befassten Mitarbeiter im Zug des rasanten technologischen Fortschritts und der damit ebenfalls einhergehenden Ausweitung des SAP-Produkt-Portfolios einen erheblichen Wandel ihrer Tätigkeiten erleben werden, ist nicht neu.

Erste Diskussionen innerhalb der DSAG-Community kamen bereits vor mehr als fünf Jahren auf und führten – wie schon eingangs erwähnt – zur Gründung einer Projektgruppe, die im Jahr 2016 die DSAG-Handlungsempfehlung „Die SAP-Basis von morgen“ veröffentlicht hat. In diesem Leitfaden wird ausführlich beschrieben, wie sich die Aufgaben der „klassischen SAP-Basis“ verändern bzw. wie sie sich idealerweise in den Unternehmen weiterentwickeln.

Der Leitfaden identifiziert ***sieben Handlungsfelder***:

- Skills und Rollen – Cloud und Supplier Management, Stärkung des Technologiearchitekten, Fokus auf Projektarbeit,
- Marketing und Selbstverständnis – Erstellung eines Servicekatalogs, regelmäßiger Austausch mit dem CIO und anderen Stakeholdern, Umbenennung der SAP-Basis
- neue Technologien und Innovation – Test- und Innovationslabor, proaktive & regelmäßige Schulungen
- Organisation im Wandel – Ausprägung der beiden Fachbereiche infrastrukturnah und anwendungsnah, virtuelle Experten-Teams
- Standardisierung und Automatisierung – Automatisierung von Routineaufgaben, Outtasking von seltenen Aufgaben
- „Cloudability“, Outsourcing & Outtasking – Beurteilung der Nutzbarkeit für die Cloud, Nutzung geeigneter Service-Formen
- IT-Roadmap – Beeinflussung der eigenen IT-Roadmap

Wir wollen an dieser Stelle nicht den Inhalt des Leitfadens wiederholen. Alles, was dort an Erfahrungen und Empfehlungen dargestellt wird, ist heute noch absolut richtig. Jeder IT-Entscheider mit Bezug zu einer SAP-Umgebung und mit Mitarbeitern, die in diesem Bereich arbeiten, sollte „Die SAP-Basis von morgen“ (und ggf. auch die dazugehörige Masterarbeit) gelesen haben.

Mit Blick auf das Thema hybrider Betrieb haben sich im Laufe der Diskussion zum Thema „People“ einige Ergänzungen und Schwerpunkte genereller Natur ergeben, die wir an dieser Stelle beschreiben wollen.

8.1 Komplexität

Natürlich gibt es in der „Marketing- und Vertriebswelt“ immer wieder Aussagen, die versprechen, mit dieser oder jener Cloud-Lösung werde es „einfacher“, man könne sich auf „Kernkompetenzen konzentrieren“ oder man erhöhe damit seine Geschwindigkeit. Diese Ziele sind in Teilbereichen tatsächlich erreichbar, aber die Wahrheit ist: Das Ganze wird komplizierter. Ein System wird genau dann komplizierter, wenn die Anzahl der Einflussfaktoren zunimmt und genau das passiert, wenn Ihre IT hybrid wird. Nun ist Kompliziertheit an sich kein Problem und jedes moderne IT-System an sich – und ein SAP-System schon ungleich mehr – ist kompliziert. Aber alle Faktoren, wie viele es auch sind, sind bekannt und beherrschbar. Für IT-Systeme gibt es daher ein Handbuch.

So betrachtet ist jede auch noch so große hybride IT-Landschaft kompliziert, aber beherrschbar. Überspitzt formuliert: Wir haben die Systeme A, B und C, dann ersetzten wir B durch D (in der Cloud) und ergänzen C um E (auf einer Cloud-Plattform), und schon steht unsere neue Landschaft. Für alles gibt es Handbücher (Dokumentation), die Funktionen sind beschrieben, wir integrieren diese Systeme und fertig – „läuft“. Unser neues Gesamtsystem ist zwar komplizierter (da mehr Faktoren), aber wir haben eine neue bzw. bessere Funktionalität gewonnen – „check“. Soweit die Sichtweise des Managements.

Das „Problem“ für das komplizierte System ist aber leider der Mensch, denn nun wird es komplex. Komplexität unterscheidet sich von der Kompliziertheit dadurch, dass mit ihr ein Grad an Unvorhersehbarkeit einhergeht. Diese entsteht daher, dass nicht alle Einflussfaktoren bekannt sind und diese Einflussfaktoren auch noch, nach nicht immer bekannten Regeln, untereinander in Wechselwirkung stehen.

Doch warum steigt die Komplexität? Natürlich werden die komplizierten Systeme von Menschen verwaltet (im Sinne von gebaut, gewartet, bedient usw.), und umso komplizierter das System, umso mehr Menschen benötigen Sie. Für ein komplexes System gibt es kein Handbuch, sondern einen Leitfaden – „here we are“.

Eine hybride Landschaft ist also komplexer, wie sie mehr Einflussfaktoren hat und weil noch mehr Menschen damit zu tun haben. Natürlich sind damit nicht nur Mitarbeiter Ihres Unternehmens gemeint, sondern auch diejenigen, die mit den „Cloud-Anteilen“ Ihrer hybriden Landschaft zu tun haben.

Welche Folgen hat das? Die Kommunikation nimmt zu und gleichzeitig erfordert die hohe Kompliziertheit ein hohes Maß an strukturierter Denkarbeit. Und das ist im Prinzip ein Widerspruch, der heute eine große Herausforderung für Mitarbeiter in der IT darstellt.

8.2 Kommunikation und „Gamification“

Die Kommunikation und Interaktion in einer, besser gesagt: für eine hybride Systemlandschaft nimmt zu, und damit ist hier nicht die technische Kommunikation zwischen Systemen gemeint. Diese nimmt selbstverständlich erheblich zu, und die damit verbundenen Herausforderungen sind oben vielfach erwähnt, sondern die menschliche Kommunikation und Interaktion.

Bei den Diskussionen wurde häufig erwähnt, dass ein Treiber hin zu den hybriden Landschaften die Fachbereiche sind, welche schneller neue Anwendungen fordern und dass eben diese Fachbereiche erheblich mehr eingebunden werden. Wenn Sie noch einmal unter Cloud-Onboarding-Team nachlesen, welche internen Stakeholder bei der Einführung eines Cloud Service beteiligt sind, erkennen Sie, wieviel Kommunikation nötig ist. Und dies setzt sich natürlich auch im Betrieb fort.

Dass Kommunikation eine der Schlüsselkompetenzen im 21. Jahrhundert ist, dürfte schon heute niemand bezweifeln. Damit ist aber nicht nur gemeint, gut kommunizieren zu können, im Sinne von „klar ausdrücken und verständlich sein“, sondern schlicht und einfach eine sehr große Anzahl von Nachrichten empfangen, verarbeiten und versenden zu können – und das synchron und asynchron über eine Vielzahl von Diensten und Medien wie E-Mail, verschiedene Messenger, Telefon, Meetings, Dokumente, Wikis oder Social-Media-Plattformen (auch im Unternehmen, z. B. SAP Jam).

An dieser Stelle wollen wir auf ein zweites Themenfeld aufmerksam machen, welches durchaus eng mit der Kommunikation verwandt ist – zumindest, wenn man in Betracht zieht, was neuro-chemisch im Gehirn des Menschen abläuft. In den letzten Jahren ist in der Unternehmenswelt der Begriff „Gamification“ aufgekommen. Gemeint ist damit laut Wikipedia: „…die Anwendung spieltypischer Elemente in einem spielfremden Kontext … Zu diesen spieltypischen Elementen gehören unter anderem Erfahrungspunkte, Highscores, Fortschrittsbalken, Ranglisten, virtuelle Güter oder Auszeichnungen.“ Es geht also im Wesentlichen um eine Motivationssteigerung durch Stimulierung des menschlichen Belohnungssystems. Das Gleiche geschieht auch bei der Kommunikation, besonders bei sozialer Kommunikation, z. B. Chat.

Das Problem mit dem Belohnungssystem ist, dass es bei entsprechender Konditionierung immer nach Stimulierung verlangt, also einen gewissen Suchtcharakter aufweist.

Wir wollen an dieser Stelle nicht beginnen, die vielfältig entworfenen und publizierten Charakteristika der Generation X, Y oder Z aufzuzählen. Fakt ist aber, dass die jungen Generationen von Mitarbeitern (und damit sind nicht nur alle unter 40 Jahren gemeint) in erheblichem Maße mehr mit „Spielen“ aufgewachsen ist und entsprechend „trainiert“ ist. Nicht umsonst macht die Computerspielindustrie weltweit

ein Vielfaches des Umsatzes von Musik- oder Filmindustrie. Und daher kommt auch der Trend zur Gamification.

Das ist an dieser Stelle erst einmal gar nicht negativ gemeint. Nachweislich verbessert Spielen die Fähigkeiten, schnell viele Inputs zu verarbeiten und zu reagieren. Entsprechend hilft das bei der Kommunikation, vor allem der Verarbeitung von viel Kommunikation, und bei der schnellen Reaktion auf Ereignisse. Die Wissenschaft sieht heute im Computerspielen viele positive Aspekte im Hinblick auf menschliche Schlüsselkompetenzen in der modernen Welt.

Trotzdem gibt es auch die andere Seite der Medaille und die besteht, überspitzt formuliert, darin, dass ein menschliches Belohnungssystem, welches relativ kontinuierliche Stimulation gewöhnt ist, einen riesengroßen „inneren Schweinehund“ darstellt, wenn es darum geht, sich hochkonzentriert in ein Thema zu vertiefen oder einzuarbeiten. Und noch etwas weiter ausgeholt: Dies führt dazu, dass in den letzten Jahren in der Öffentlichkeit immer öfters ein Phänomen auftaucht bzw. thematisiert wird, welches schon länger bekannt und an sich nichts Neues ist – die Prokrastination. Das extreme Aufschieben von Tätigkeiten, oft zugunsten der Ausführung von leichten und/oder schnellen Tätigkeiten. Man kennt das: „… noch schnell diese E-Mail beantworten …, anfangen lohnt ja nicht, weil in 20 Minuten Pause ist …, lieber erst mal noch die Intranet-News lesen, könnte ja wichtig sein … usw.“ In Wikipedia steht: „Die Störung wird insbesondere bei Personen beobachtet, die überwiegend selbstbestimmt arbeiten…“. Doch genau das sind immer öfters die Anforderungen an modernes Arbeiten – selbstbestimmt, selbststrukturiert, eigenständig.

Dabei möchten wir auch klarstellen: Jeder Mensch ist anders und alle hier beschriebenen Erfahrungen und Tendenzen sind keinesfalls zu pauschalisieren.

8.3 Geschwindigkeit und Volatilität

Jeder in der IT-Industrie (und nicht nur dort) klagt über die zunehmende Geschwindigkeit im beruflichen Umfeld. Keine Keynote kommt heute ohne die berühmten Hockey-Kurven aus. Man kennt das ja: „Sehen Sie hier … das Auto, das Telefon, das iPhone und dann Pokemon Go – unfassbar“. Es ist eigentlich schon ein bisschen lustig. Auffälligerweise zeigen diese Kurven ausnahmslos Dinge aus der Consumer-Welt. Natürlich machen die heutige weltweite Vernetzung und die verfügbare Anzahl von Konsumenten und deren Einkommen solche exponentiellen Wachstumsraten möglich. Bei Produkten und Dienstleistungen für Unternehmen sieht die Sache logischerweise etwas anders aus. Welches IT-Unternehmen träumt nicht von solchem Wachstum – und davon ist auch SAP mit seinen Cloud-Produkten nicht ausgenommen. In Unternehmen treffen neue Produkte, Lösungen und Services logischerweise auf Strukturen, und das macht die Adaptionsgeschwindigkeit an irgendeiner Stelle endlich.

Selbstverständlich haben das Wachstum und die Geschwindigkeit Auswirkungen auf alle Unternehmen, denn am Ende der Kette steht direkt oder indirekt immer ein Endkunde, und daher steigt auch der Druck auf die Handlungsgeschwindigkeit und die Anforderungen an die interne IT. Die Konsequenz, die heute alle IT-Mitarbeiter spüren, ist schlicht eine steigende Anzahl von Projekten und permanenter Veränderungs- und Anpassungsdruck. Der IT-Mitarbeiter von heute und morgen ist in einem dauerhaften Projektmodus und arbeitet in der Regel an mehreren Projekten parallel bzw. ist an ihnen beteiligt.

Die zunehmende Geschwindigkeit führt zu einem weiteren Problem, das dem Menschen von Natur aus zu schaffen macht – Volatilität. Gemeint ist hier das Phänomen des „Moving Target“, bedingt durch mehrere Einflüsse und Faktoren:

- Anforderungen ändern sich innerhalb eines Projekts.
- Rahmenbedingungen ändern sich während der Projektlaufzeit.
- Umso komplizierter Systeme sind, umso schwieriger und aufwändiger sind Spezifikationen eines angestrebten Endzustands, also geht man hier Kompromisse ein.

Natürlich gibt es Anforderungen und Rahmenbedingungen, die dem entgegenwirken. Man denke nur an die Stichworte Compliance, Gesetze, Zertifizierungen in kritischen Bereichen (Medizin, Verkehr usw.) und einige mehr. Am Ende kosten diese Zeit und Geld und erhöhen die „innere Spannung“ im Unternehmen zwischen Anforderungen und Machbarkeit.

Die Antwort auf „Geschwindigkeit und Volatilität“ ist – wer hat es nicht schon gehört? – Agilität, also die Gewandtheit, Wendigkeit oder Beweglichkeit von Organisationen und/oder Personen bzw. in Strukturen und/oder Prozessen. Ein Riesenthema der letzten Jahre in der IT. Jeder kennt die Begriffe agile Entwicklung, DevOps, SCRUM, usw. Doch auch die Anpassung der IT auf diese neuen Methoden, um sie besser auf die Herausforderungen einzustellen, ist für sich schon eine wirklich riesige Aufgabe – ein bisschen SCRUM funktioniert nicht!

Dies erfordert von den Mitarbeitern Veränderungen und Anpassungen – das Thema Change Management in Organisationen ist endlos, und trotzdem muss man sich dem stellen.

8.4 Fokussierung und Selbstorganisation

Wenn man heute in die modere Arbeitswelt von IT-Mitarbeitern schaut, so erkennt man, dass es die entscheidende persönliche Herausforderung für den Mitarbeiter ist, den Wechsel zwischen hochkommunikativen und hochkonzentriertem Arbeiten zu bewältigen.

Der Wechsel in das kommunikative Arbeiten fällt (fast) jedem leicht, denn der Mensch ist ein kommunikatives Wesen und es bedarf dazu keinerlei Anstrengung oder Vorlauf. Der Wechsel in ein hochkonzentriertes Arbeiten ist dagegen eine echte Herausforderung und erfordert Fokussierung und Selbstorganisation.

Wir wollen an dieser Stelle das Thema Fokussierung nicht vertiefen. Das ist eine sehr individuelle Herausforderung und es gibt unzählige Ratgeber dazu und zu all den angrenzenden Bereichen wie Konzentration usw.

Die Selbstorganisation, oder besser gesagt, eine gute Selbstorganisation des Mitarbeiters ist enorm wichtig, um die zuvor beschriebenen Herausforderungen zu bestehen. Sie werden sagen, dass dies nichts wirklich Neues ist und dass es natürlich schon immer so war, dass ein, nennen wir es einmal anders, strukturiertes Arbeiten wichtig und in der Regel auch erfolgreicher ist. Aber aufgrund der eingangs beschriebenen Herausforderungen (Komplexität, Geschwindigkeit, Kommunikation usw.) ist für eine erfolgreiche Organisation oder Abteilung heute umso mehr essentiell, dass ihre Mitglieder ein hohes Maß an Selbstorganisation mitbringen.

Jeder Mitarbeiter in der IT ist heute sein eigener Multi-Projektmanager!

Haben Mitarbeiter diese Selbstorganisation nicht in ausreichendem Maß, werden diese sich kaum oder selten die Freiräume „erkämpfen“, um fokussiert und hochkonzentriert an einem komplizierten System oder einem komplexen Problem zu arbeiten. Sicher kennen Sie Kollegen, die nie so richtig mit etwas fertig werden und denen man im Prinzip täglich sagen muss, was sie tun sollen – Stichwort Micro-Management. Eigenartigerweise sind das oft die Kollegen, welche auf eine E-Mail unmittelbar reagieren oder die bei einer Bitte um konkrete kurzfristige Unterstützung immer Zeit haben (was tatsächlich auch mal ein Vorteil sein kann).

Jeder aktuelle Management-Ratgeber wird Ihnen sagen, dass Micro-Management komplett von gestern und auch sonst einfach schlecht ist. Die Zukunft ist eigenverantwortliches und selbstorganisiertes Handeln von Mitarbeitern und Teams. Die Wahrheit ist aber auch, dass es dafür Fähigkeiten braucht, und die hat nicht jeder und die erlernt auch nicht jeder. Nicht falsch verstehen, natürlich ist das der einzig richtige Weg für die Zukunft, aber einfach ist und wird es nicht!

8.5 Training

Wenn Sie beginnen, Cloud-Anwendungen in Ihre Landschaft zu integrieren, also der hybride Betrieb beginnt, steht natürlich unmittelbar die Frage nach Trainings- und Schulungsangeboten im Raum.

Wir beschreiben in diesem Kapitel ja weniger die fachlichen als persönlichen Herausforderungen, aber trotzdem ist natürlich das fachliche Wissen der Mitarbeiter die absolute Grundlage für ein erfolgreiches Projekt oder einen erfolgreichen hybriden Betrieb. Wenn Sie also vor einem solchen Projekt stehen, planen Sie die

entsprechenden Trainings und Schulungen für die zu integrierende Lösung ein. Alles andere wäre fahrlässig. Für viele Cloud-Angebote von SAP gibt es Schulungen, die den Integrationsaspekt zu den On-Premise-Lösungen im Fokus haben. Diese können eine gute Unterstützung sein.

Die Trainings und Ausbildungen sollten Sie an dem neuen Rollenkonzept orientieren, welches in der DSAG-Handlungsempfehlung „Die SAP-Basis von morgen“ beschrieben ist. Dabei sollten Sie auch größere Zusammenhänge im Auge haben als nur die eine neue Cloud-Anwendung, um die es vielleicht im aktuellen Projekt geht. Eine besonders wichtige Rolle kommt hier dem Technologiearchitekten zu, und entsprechend müssen Sie in dieses Know-how investieren. Im Idealfall hat die HR-Abteilung Ihres Unternehmens bereits ein Konzept und eine Strategie für die individuelle Weiterentwicklung Ihrer Mitarbeiter, dann können und sollten Sie diese nutzen, um die neuen Rollen nach und nach im Team zu etablieren.

Neben den fachlichen Aspekten, sind die hier in diesem Kapitel beschriebenen Soft Skills von entscheidender Bedeutung für den Erfolg in der hybriden Zukunft und natürlich auch im peziellen beim hybriden Betrieb. Was läge also näher, als auch diese zu trainieren? Natürlich ist völlig klar, dass Sie mit einem solchen Anliegen vermutlich nicht weit kommen werden. Wenn Sie einen Projektplan für die Einführung einer Cloud-Lösung inklusive hybridem Betrieb vorlegen sollen und dort ein Training für Selbstorganisation einplanen, werden Sie das sicher nicht durchbekommen. Verständlicherweise, denn diese Fähigkeiten sind ja auch nicht projektspezifisch. Sie brauchen also auch hier die HR-Abteilung und sollten diese dafür sensibilisieren, vor welchen Herausforderungen Ihre IT-Mitarbeiter und -Kollegen stehen. Die Alternative sind schlicht weitere oder andere Mitarbeiter, die die nötigen Fähigkeiten mitbringen. Ein sehr schweres und/oder sehr teures Unterfangen in Zeiten des Fachkräftemangels.

Last but not least benötigen die Mitarbeiter natürlich die Freiräume, um sich aus- und weiterzubilden. So logisch dies jedem erscheinen mag, so zeigt die Erfahrung, dass es heute gerade daran oft mangelt. Die hohe Projekt- und Arbeitslast macht die Umsetzung dieser einleuchtenden Notwendigkeit immer schwieriger.

Um es hier klarzustellen: Das Erlernen von Neuem, was ja der Sinn von Schulungen und Trainings ist, ist hochkonzentriertes und kein hochkommunikatives Arbeiten. Neues Wissen muss erarbeitet werden, und das gelingt nicht, wenn die Aufmerksamkeit durch E-Mail oder andere Kommunikation gestört wird. Auch diese Art von Freiraum braucht es.

8.6 Fazit

Zum Abschluss dieses etwas anderen Kapitels wollen wir noch einmal auf die DSAG-Handlungsempfehlung „Die SAP-Basis von morgen“ hinweisen – bitte lesen Sie diese.

Der unserer Meinung nach entscheidende Faktor für den erfolgreichen hybriden Betrieb ist der Mensch, der Mitarbeiter. Er muss die Herausforderungen bewältigen und benötigt daher Unterstützung in Form von Freiraum für das Neue und Motivation durch Training von Hard- und Softskills sowie Anerkennung.

Forderungen an SAP im People

- Hier mal keine ☺

Versteckte Kosten

- Der Betrieb von hybriden Landschaften ist bestenfalls kostenneutral zu einem reinen On-Premise-Betrieb, i.d.R. ehr teurer, da komplizierter, komplexer und mit neuen und zusätzlichen Anforderungen verbunden.
- Wenn Mitarbeiter sich nicht in den Betrieb einer hybrider IT voll einbringen können oder wollen, benötigen sie zusätzliche Ressourcen mit entsprechenden Fähigkeiten.

APPENDIX

Glossar

Allgemeine Begriffe – Abkürzungen	
Capex	Investitionsausgaben
CSA	Cloud Controls Matrix
DMZ	Demilitarized Zone
E2E-BPM	End-To-End Business Process Monitoring
IAM	Identity and Access Management
IDM	Identitiy Management
ITSM	IT Service Management
Opex	Betriebskosten
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

Leistungsschein 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 agreemend
	Service Area Service Sub Area Service Description	Description of Service and Sub-service Area and short description of respective Sercice
	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	X		yes

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
			SAP recommendations and CUSTOMER needs			
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 affects 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 according to security policies		X	no
1	62	SAP system administration	Manage SAP end-user accounts according to security policies		X	no
1	63	SAP system administration	Manage SAP end-user accounts password reset according to 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

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
1	66	SAP system administration	Maintain customer accounts for FTP, SFTP or NFS, Samba shares, incl. creation of new shares	X		no
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 Roles and Authorizations team		X	no
1	68	SAP system administration	Manage SAP OSS customer user accounts and developer's 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 according to 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 according to 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. Filesystem, 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

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
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
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

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
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
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 of 3rd party providers (eg. 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

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
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 upcomming versions of this document			no
3	0	SAP system monitoring	**SAP SYSTEM MONITORING**			
3	1	SAP system monitoring	Setup, install, configure and test monitoring environment and tools used by Service Provider	X		yes
3	2	SAP system monitoring	Setup, 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 Backend 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) according to VENDOR standards	X		no
4	6	SAP system setup	Set up high availability solution for SAP system instances selected by CUSTOMER	X		no

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
4	7	SAP system setup	Create CUSTOMER SAP system clients, setup clients parameters according to CUSTOMER specifications	X		no
4	8	SAP system setup	Setup SAP system Change Option according to CUSTOMER specifications (Transaction SCC4)		X	no
4	9	SAP system setup	Define and setup 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
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 setup workload distribution Logon Load Balancing, SAP Logon Groups		X	no
4	14	SAP system setup	Setup workload distribution on SAP Web Dispatcher	X		yes
4	15	SAP system setup	Define and setup 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	Setup and enable Service Provider Standard monitoring of the system(s)	X		no
4	19	SAP system setup	Setup 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) according to 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

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
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**			
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 data base performance troubleshooting	X		yes
5	21	Database administration	Database performance tuning on the system level (i.e. 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 on the 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 (i.e., 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 (i.e. indexes, tables) on request following change management procedure	X		no
5	27	Database administration	Supporting CUSTOMER during Audits, e.g. providing information, describe processes, run scripts	X		no

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
6	0	Database monitoring	**DATABASE MONITORING**			
6	1	Database monitoring	Setup, 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
6	5	Database monitoring	Respond to events following the notification/escalation procedure	X		yes
6	6	Database monitoring	Monitor the database grow 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

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
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, according to 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
9	5	Database security	Notify about changes to security policies or any discovered security leaks	X	X	yes
10	0	HANA Special AddOns	**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 AddOns	**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

Sec.	ID	Service Sub Area	Service Description	A Responsibility	Customer Responsibility	Included
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 adaption	X		yes
11	14	Configuration	BEX Query	X		no
11	15	Operation	SolMan related tasks when decommisioning a System	X		yes
11	16	Operation	SolMan related tasks when patching a Satelite System	X		yes
11	17	Operation	SolMan SPS patching Post Action	X		no
11	18	Operation	Update SLD CIM model/CR content	X		yes

Legende zur Verantwortlichkeitsmatrix:

D — Durchführung (R Responsible) – verantwortlich für die Durchführung. Die Partei oder Parteien, die die Aktivität/Tätigkeit durchführt/-en.

V — Verantwortlich (A Accountable) – verantwortlich im Sinne von „genehmigen“. Die Partei, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt.

M — Mitwirkung (C Consulted) – liefert zusätzliche, meist fachliche Informationen. Die Partei oder Parteien, die durch zusätzliche, meist fachliche Informationen bei der Durchführung der Aktivität bzw. Tätigkeit mitwirken soll/sollen.

I — Information (I Information) – zu informieren. Die Partei oder Parteien, die über den Verlauf bzw. das Ergebnis der Tätigkeit zu unterrichten ist/sind bzw. die berechtigt ist/sind, die entsprechende Information zu erhalten.

F — Freigabe – Die Partei oder Parteien, die eine Aktivität vorab genehmigen muss/müssen, bevor diese durchgeführt werden darf.

P — Projekt – Optionaler Service, Lieferung im Rahmen von bei Service Provider beauftragten Projekten.

APPENDIX B: SAP Service Parameter

B. Basisbetrieb SAP (Basisbetrieb)

B.1 Bereitstellung von Services

Für die Services im Bereich des SAP- Betriebs werden die nachfolgenden Erledigungszeiten bis zur Bereitstellung der Services vereinbart.

Priorität	Erledigungszeit
Priorität 1 (Critical)	8 h
Priorität 2 (Major)	3 Arbeitstage
Priorität 3 (Standard)	10 Arbeitstage
Priorität 4 (Request)	20 Arbeitstage

Kategoriebeispiele der Services:

Priorität 1: Einzelner Hinweis-Einbau, Einrichtung Drucker, Recovery-Clone

Priorität 2: Print-Server, Berechtigungs-Änderungen, Erstellung Transaktionen, Job-Anforderungen und Job-Änderungen

Priorität 3: Erstellung Test-System, Installation SAP-Add-On in Entwicklungs- oder Test-Umgebung

Priorität 4: Installation neues SAP-Produktions-System, Installation Hot Packages, Austausch SAP-Kernel in gesamter Landscape

Während der Transitionsphase erfolgt eine Kategorisierung der Services.

B.2 Systemverfügbarkeit

„Platin“-Anwendungsverfügbarkeit für alle produktiven SAP-System-Landschaften (komplette Landscape), inkl. Subkomponenten (z. B. LiveCache, BWA etc.)

„Bronze“-Anwendungsverfügbarkeit für alle Test-SAP-System-Landschaften (Sandbox- Systeme), inkl. Subkomponenten (z. B. LiveCache, BWA etc.)

„Platin“-Anwendungsverfügbarkeit für alle produktiven Non-SAP-Komponenten (z. B. MQ Series, Content Manager, Business Connector, Vertex, Dollar Universe etc.)

Max. Anzahl zulässiger Ausfälle pro Jahr: siehe Pkt. 3. Data Center Services Messkriterien für die Systemverfügbarkeit der SAP-Systeme:

- Logon-Check in jedem System
- Verbucher muss in jedem System aktiv sein
- Sperrverwaltung muss in jedem System funktionsfähig sein

Messkriterien für die Systemverfügbarkeit der Non-SAP-Systeme:

- SAP-Schnittstelle muss funktionsfähig sein
- Individuelle Prüfroutinen über Tools, Stand heute: SAP SolMan und /oder Nagios je nach System (z. B. Dollar Universe, MQ Series)

Die SAP Application Server und Datenbank-Server sind ohne gesonderte Servicezeiten für Standard-System-Wartungsarbeiten (z. B. Datenbank- und Betriebssystem Patch, SAP Kernel Upgrade) zu betreiben. Der Einbau erfolgt im Customer Standard durch Failover-Mechanismen ohne Unterbrechung des SAP-Betriebs.

B.3 Antwortzeiten

Die SAP-Antwortzeiten werden anhand der in der Transaktion ST03N dargestellten Response Time Distribution (inkl. Dialog Time) gemessen. Hierbei wird der gemittelte Monatswert aller Instanzen anhand der kumulierten, prozentualen Verteilung betrachtet. Relevant ist die Quote der Transaktionen, die eine Antwortzeit von <0,1s, <0,5s und <1s erreichen. Ebenfalls betrachtet wird für bestimmte Transaktionstypen der maximale Stundendurchschnitt während der Online-Peek-Zeit, dargestellt in der Transaktion ST03N im Time Profile. Die Online Peek-Zeit gilt für die Stunde mit den meisten Transaktionen je Transaktionstyp pro Stunde im jeweiligen System.

Die durchschnittlichen Antwortzeiten der SAP-Systeme werden gemäß der folgenden Tabelle festgelegt, die den heutigen Stand der Systeme plus einen Puffer von ca. 10% widerspiegeln:

		< 0.1s	< 0.5s	< 1s	Peek 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**	**Peek 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	Peek 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	Peek 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	Peek 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	Peek 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	Peek 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	Peek 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	Peek 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	Peek 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	Peek 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

Werden diese Antwortzeiten in einem Monat nicht erreicht, so müssen Analysen und geeignete Maßnahmen eingeleitet werden, die dazu führen müssen, die Antwortzeit zu verbessern. Wird die Antwortzeit in zwei aufeinanderfolgenden Monaten nicht erreicht, gilt das SLA als nicht erfüllt.

Die Antwortzeiten der SAP-Development, SAP-Konsolidierungssystem und SAP-JAVA-System sowie der Non-SAP-Systeme müssen mindestens dem heutigen Standard entsprechen und dürfen die SAP-Funktionalität für die Anwender nicht beeinträchtigen.

B.4 Deadlines für Batch-Verarbeitung

Für die Batch-Verarbeitung müssen folgende Zeitfenster und Deadlines eingehalten werden, sofern keine Job-Abbrüche o.ä. auftreten:

PE1, PG1, PA1, PP1, PM1	Nacht-Batch-Kette bis 7:00h lokaler Zeit fertig PE1,
PG1, PA1, PP1, PM1	Tägliche Sicherung bis 23:30h lokaler Zeit fertig PE1,
PG1, PA1, PP1, PM1	BW Trigger Event bis 06:00h lokaler Zeit fertig
PW1	Datenübernahme aus ERP-Systemen bis 8:00h fertig

Während der Transitionsphase erfolgt ggf. die Aufnahme von weiteren Deadlines.

B.5 Fehlerbehandlung und Fehlerbehebung

Es gelten folgende Störungsbehebungszeiten:

Incident Priorität 0 (Auto-Reaktion)	1-10min (je nach Automation)
Incident Priorität 1 (Critical) Incident	2h
Priorität 2 (Major)	8h
Incident Priorität 3 (Standard)	24h
Incident Priorität 4 (Request)	48h

Für die kritischen Business-Prozesse gelten die Einstufungen der Fehlerpriorität. Es muss ein VIP Support gewährleistet werden (z. B. Yellow Book im BW für Geschäftsleitung, HR für Geschäftsleitung, Störungen bei VIPs).

Für die im heutigen Customer Standard bereits mit Hilfe von Automationsprozessen festgelegten Auto-Reaktionen gilt die Priorität 0 (z. B. File System Überwachung, Datenbank Restart bei Abbruch, automatische Reaktion auf Hardware-Ausfälle, automatische SAP-Datenpool-Vergrößerung bei Erreichung von 95% Füllgrad etc.). Die Automatismen sind für die Sicherstellung des 7x24-SAP-Betriebes notwendig.

Während der Transitionsphase erfolgt die Festlegung der Eskalationsszenarien.

Impressum

Wir weisen ausdrücklich darauf hin, dass das vorliegende Dokument nicht jeglichen Regelungsbedarf sämtlicher DSAG-Mitglieder in allen Geschäftsszenarien antizipieren und abdecken kann. Insofern müssen die angesprochenen Themen und Anregungen naturgemäß unvollständig bleiben. Die DSAG und die beteiligten Autoren können bezüglich der Vollständigkeit und Erfolgsgeeignetheit der Anregungen keine Verantwortung übernehmen.

Deutschsprachige SAP® Anwendergruppe e.V.
Altrottstraße 34 a
69190 Walldorf | Deutschland
Telefon +49 6227 35809-58
Telefax +49 6227 35809-59
E-Mail info@dsag.de

dsag.de