devoteam

Cloud **Computing**

Im US/FDA und EU/GMP -
regulierten Umfeld

Creative tech for Better Change

INHALT.

1 MANAGEMENT SUMMARY.

Mit Cloud Computing die IT-Kosten senken – dieser Satz ist das Kernargument der Befürworter der Cloud. Tatsächlich setzen immer mehr Unternehmen, vom Großkonzern bis zu klein- und mittelständischen Unternehmen, auf „die Wolke".

Kann dieser Weg auch für die streng regulierten IT-Systeme in der Pharma- und Medizintechnik-Industrie beschritten werden?

Insbesondere für Anwendungen und Daten, die einen Einfluß auf Patientensicherheit, Produktqualität und Datenintegrität haben, gelten neben den Anforderungen an physikalische, technische und logische Sicherheit zusätzliche Anforderungen, die durch die Zulassungs- und Aufsichtsbehörden für Pharma- und Medizintechnik-Produkte festgelegt sind.

Aus den bestehenden Richtlinien und Gesetzen lassen sich Vorgehensweisen ableiten, die es regulierten Unternehmen ermöglichen, den Weg in die Cloud zu definieren.

Die Aufgaben und Tätigkeiten des regulierten Unternehmens im Rahmen eines Cloud-Projektes werden beschrieben und bewertet.

Die Anforderungen an den Service Provider werden ebenfalls abgeleitet und dokumentiert.

2 CLOUD COMPUTING – VERSUCH EINER DEFINITION.

2.1 Begriffsbestimmung

Laut der US-amerikanischen Standardisierungsstelle NIST (National Institute of Standards and Technology) ist Cloud Computing wie folgt definiert:

> *Cloud Computing ist ein Modell, das es erlaubt* bei Bedarf, jederzeit und überall *bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste)* zuzugreifen, *die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können.*

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) bezieht sich ebenfalls auf diese Definition. Zusätzlich sind folgende Eigenschaften zusammengefasst definiert:

1. On-demand Self-Service
   Der Zugriff auf den Dienst und die Provisionierung der Ressourcen erfolgen automatisch, ohne Interaktion mit dem Cloud Anbieter. Niemand muss beim Anbieter manuell etwas zur Verfügung stellen, mit Ausnahme der Ersteinrichtung.
2. Broad Network Access
   Der Dienst wird über das Internet mit Standard-Mechanismen zur Verfügung gestellt und kann mit verschiedenen Endgeräten genutzt werden.
3. Resource Pooling
   In aller Regel wird der Dienst nicht exklusiv einem Anwender zur Verfügung gestellt, sondern einer Vielzahl Nutzern, die sich das Angebot teilen.
4. Rapid Elasticity
   Der Anwender nutzt den Dienst, der ihm je nach Anwendungsbedarf bezüglich der benötigten Ressourcen flexibel zur Verfügung gestellt wird.
5. Measured Service
   Die Nutzung der Ressourcen des Cloud-Dienstes kann gemessen und überwacht werden und in Form einer Abrechnung zur Verfügung gestellt werden.

2.2 Bereitstellungsarten und Modelle

Cloud-Dienste können in verschiedenen Formen zur Verfügung gestellt werden. Am bekanntesten ist die Public Cloud, die von Anbietern wie Google, Amazon und anderen dem Anwender zur Verfügung gestellt werden. Die Dienste sind offen über das Internet verfügbar. In der Regel hat der Anwender keinen Einfluß auf die Implementierung und den Betrieb der Cloud-Dienste.

Im Gegensatz dazu handelt es sich bei der Private Cloud um eine Form von Cloud-Diensten, bei denen der Zugriff auf einen klar definierten Personenkreis beschränkt ist, der Betrieb entweder im Unternehmen selbst verbleibt oder auf einer dezidierten Infrastruktur bei einem Hosting Provider abgebildet wird. Innerhalb dieser Infrastruktur haben die zur Verfügung gestellten Dienste jedoch die Flexibilität einer Cloud.

Daneben gibt es noch weitere Ausprägungen und Mischformen der Bereitstellungsarten. In Abbildung 1 sind diese aufgeführt und in ihren Eingenschaften gegenübergestellt.

Abbildung 1: Bereitstellungsarten in der Cloud

Aufbauend auf den beschriebenen Bereitstellungsarten können verschiedene Cloud Service-Modelle als Cloud-Dienst in Anspruch genommen werden.

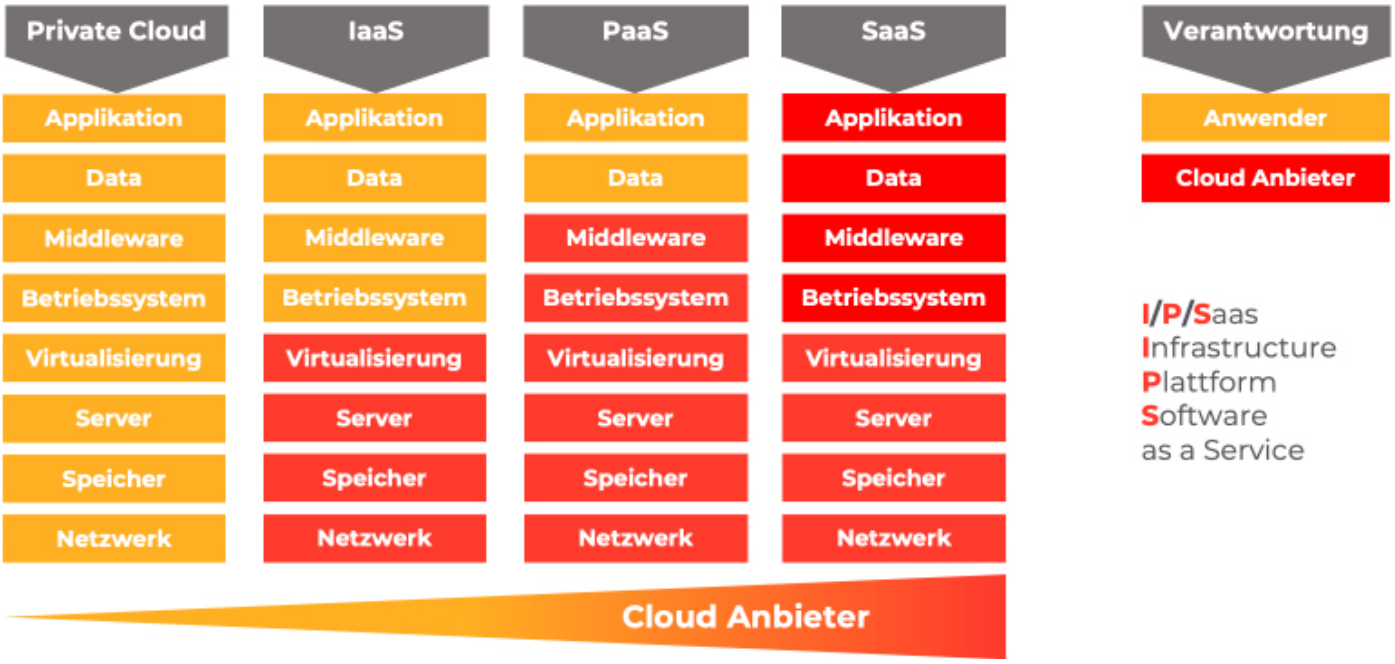


Abbildung 2: Service-Modelle und Verantwortung

Im Fall von „Infrastructure as a Service" werden klassische IT Infrastruktur Komponenten (Rechenleistung, Speicher, Netzwerk, Virtualisierungsumgebung) als Dienst angeboten. Es handelt sich in der Regel um hochstandardisierte Services, auf denen der Kunde dann unter seiner Kontrolle und Verantwortung ab dem Betriebssystem der virtuellen Server seine Anwendungen implementiert und betreibt.

Im Fall von „Platform as a Service" wird über die Virtualisierungsumgebung hinaus eine Plattform (Middleware, z.B. SAP, SharePoint) zur Verfügung gestellt, auf der der Kunde nur Zugriff auf seine plattformbasierten Applikationen hat. Die Plattform selbst wird mandantenfähig und skalierbar zur Verfügung gestellt.

Ein Spezialfall im Rahmen der Cloud Service-Modelle stellt „Software as a Service" dar. Hier agiert der Cloud Service Provider bis in die Applikationsebene. Der Kunde gibt hier die gesamte Kontrolle bis einschließlich zur Anwendung an den Cloud Service Provider ab.

Der Cloud-Kunde kann zwar je nach gewähltem Service-Modell Aufgaben an den Cloud Service Provider delegieren, nicht aber die Verantwortung für die Einhaltung der für ihn geltenden Compliance-Anforderungen, seien sie intern oder durch den Gesetzgeber formuliert!

Einen weiteren Sonderfall stellt auf der anderen Seite der Skala die Private Cloud dar. Hier verbleibt die gesamte Infrastruktur bis zur Applikation beim Kunden in einem internen Rechenzentrum. Die Vorteile der Cloud werden hier intern über eine Virtualisierung und Standardisierung der Managed Services ermöglicht.

2.3 Virtualisierungskonzepte für Cloud Computing

Insbesondere vor dem Hintergrund der Einhaltung von Compliance-Anforderungen ist im Rahmen von Cloud Computing eine klar definierte und technisch realisierte Trennung von Mandanten auf Applikationsebene erforderlich. Für deren Umsetzung können verschiedene Virtualisierungskonzepte herangezogen werden.

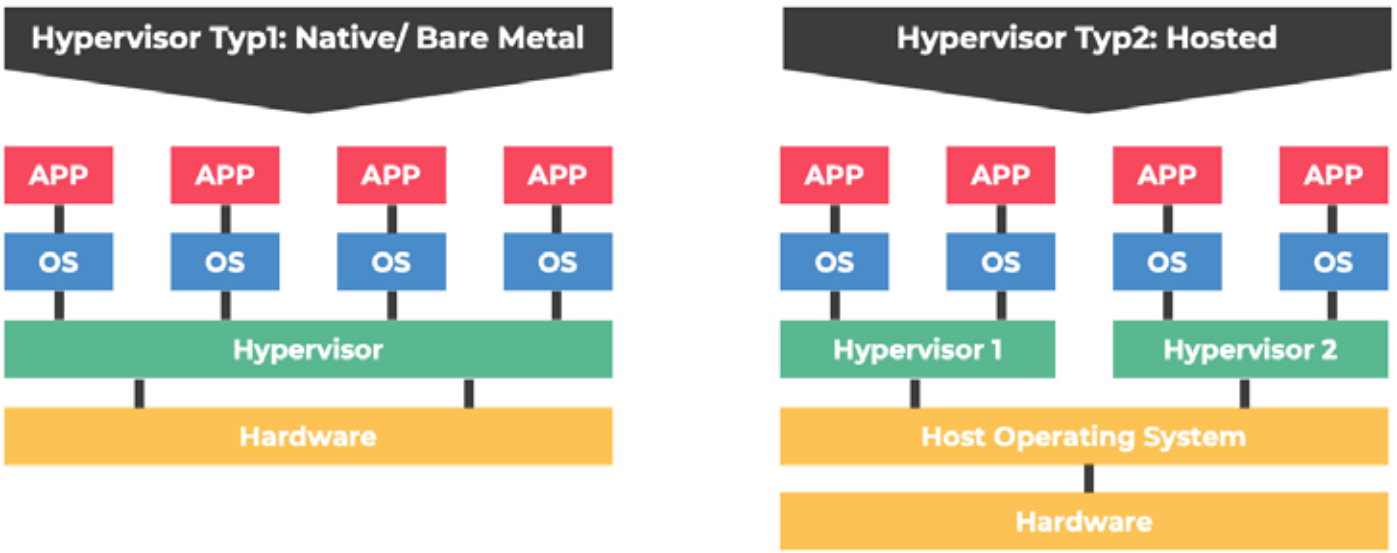


Abbildung 3: Virtualisierungskonzepte

Auf der Grundlage des Konzeptes „Hypervisor Typ 2“ in Abbildung 3 ist eine solche Trennung technisch einfach umsetzbar.

2.4 Software as a Service – Private Cloud basierte Portale für klinische Studien

Lange bevor Cloud Computing in aller Munde war, wurden für klinische Studien zentrale, mandantenfähige Software-Lösungen angeboten, die alle anfallenden Daten aus Klinik, Labor und klinischem Datenmanagement integrieren und den vollständigen Lebenszyklus und Datenmanagementprozess einer klinischen Studie komplett als „End-to-End"-Prozess abdecken [1]. Dank der durchgängigen Nutzung der verschiedenen CDISC-Standards vom CRF-Design über Datenerfassung, Datenbereinigung (Data Cleaning) und Datenexport bis zur Tabulation, Auswertung und Archivierung entfallen Medienbrüche, manuelle Prozessschritte und damit Datenumwandlungsfehler [2,3].

Diese Software wird über ein oder mehrere dedizierte Rechenzentren als Software as a Service in einer Private Cloud zur Verfügung gestellt.

Diese Services werden von Pharma- und Medizintechnik-Unternehmen intensiv genutzt und sind Bestandteil behördlicher Audits. Für die Sicherstellung der hier notwendigen Konformität mit GCP- und US FDA 21 CFR Part 11/ EU GMP Annex 11 werden die Anbieter dieser Services intensiv auditiert. Neben dem Qualitätsmanagement, dem Software Lifecycle und der Qualifizierung der Cloud-Infrastruktur steht die Eignung des Rechenzentrums für das Hosting der Software insbesondere unter den Aspekten von physikalischer, technischer und logischer (Datenintegrität und Datenvertraulichkeit) Sicherheit im Fokus.

3 ANFORDERUNGEN DER BEHÖRDEN.

Wirft man einen Blick in die für Pharma- und Medizintechnik-Unternehmen sowie für klinische Studien geltenden Richtlinien, Gesetze und Normen, stellt man sehr schnell fest, dass sich in den US FDA 21 CFR Part 210, 211,820, dem EU GMP-Leitfaden, den GCP-Richtlinien oder der DIN EN ISO 13485 nur sehr wenig Konkretes bezüglich der IT-Systeme findet. Es lässt sich aus ihnen jedoch richtigerweise ableiten, dass hier eine Konformität zum US FDA 21 CFR Part 11 oder EU GMP Annex 11 zwingend erforderlich ist. So heißt es im Annex 11 grundsätzlich:

> *Annex 11 applies to all forms of computerised systems used as part of a GMP regulated activities. ... The application should be validated; IT infrastructure should be qualified.* [4]

Darüber hinaus existieren für Cloud Computing noch keine spezifischen regulatorischen Anforderungen seitens der Behörden. Eine Orientierung an den bestehenden Vorgaben und deren Interpretation für Cloud Computing ist aktuell ein gangbarer Weg. Hilfreich sind hier auch GAMP Good Practice Guides, z.B. Testing, in dem sich bereits Definitionen für das Cloud Umfeld finden lassen.

Hierbei sind neben dem Annex 11 noch die Kapitel 4 (Documentation) und 7 (Outsourced Activities) des EU GMP-Leitfadens sowie die Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) relevant.

Grundlegend ist die Frage, ob Dokumentationen im Sinne der AMWHV, des AMG und den GMP-Richlinien außerhalb der von der Herstellerlaubnis erfassten Räumlichkeiten – und diese sind innerhalb der Gebäude des regulierten Unternehmens – aufbewahrt werden dürfen. In der AMWHV heisst es in §20 (1):

> *Die Aufbewahrung muss in einem geeigneten Bereich der von der Erlaubnis nach § 13 oder § 72 des Arzneimittelgesetzes erfassten Räume erfolgen. Die Zugriffsberechtigung zu den Aufzeichnungen nach Satz 1 ist durch geeignete Maßnahmen auf dazu befugte Personen einzuschränken. Für den Fall einer Schließung des Hersteller- oder Prüfbetriebs, in dem die Aufbewahrung der Dokumentation nach Satz 1 erfolgt, hat der pharmazeutische Unternehmer Vorsorge zu treffen, dass die Dokumentation während der gesamten Aufbewahrungszeit vorgehalten wird.*

Das Votum der Expertenfachgruppe 11 (EFG 11, V11002) beantwortet diese Frage zwar mit einem „ja“, formuliert aber sehr konkrete Anforderungen, die es umzusetzen gilt. Die Eignung und Kompetenz des Dienstleisters, in dessen Räumen diese Systeme implementiert und betrieben werden, gilt es, dokumentiert und für die Behörden transparent zu prüfen und zu überwachen. Dabei wird die Qualifizierung und Validierung dieser Systeme als zwingend erforderlich angesehen. Maßnahmen zur Sicherstellung von Verfügbarkeit, Richtigkeit, Vollständigkeit und Lesbarkeit der Daten muss man vertraglich mit dem Dienstleister fixieren.

Die wesentlichen Anforderungen sind in Tabelle 1 zusammengefasst. Für jedes Projekt, in dem es um die Auslagerung von regulatorisch relevanten Daten und Dokumenten in die Cloud geht, sind diese Anforderungen als Bestandteil von Planung und Umsetzung festzulegen.

Anforderung	Referenz
Die IT-Systeme müssen (ausreichend) validiert sein	AMWHV §10 EU GMP Annex 11 US FDA 21 CFR Part 11
Daten müssen entlang der Aufbewahrungsfrist verfügbar sein	AMWHV §§ 10,20 EU GMP Annex 11, 7.1 EU GMP Leitfaden Kap. 4 US FDA 21 CFR Part 11
Zugriff auf Daten muss für einen unverzüglichen Rückruf schnell möglich sein	AMWHV §10 Votum EFG 11 (V11002)
Gespeicherte Daten müssen gegen Verlust und Beschädigung geschützt sein	AMWHV §10 EU GMP Annex 11, 7.1
Zugriff auf Daten muss auf befugte Personen beschränkt sein	AMWHV §10
Formale Vereinbarungen zur Regelung von Verantwortlichkeiten von Lieferanten und Dienstleistern	EU GMP Annex 11, 3.1
Nachweis der Kompetenz und Zuverlässigkeit des Lieferanten durch regelmäßige Audits und Überprüfungen	EU GMP Annex 11, 3.2 EU GMP Leitfaden Kap. 7
Informationen zu Qualitätssystem und Audits müssen den Behörden auf Nachfrage zur Verfügung gestellt werden	EU GMP Annex 11, 3.4
Verfügbarkeit, Lesbarkeit und Richtigkeit gespeicherter Daten ist zu prüfen	EU GMP Annex 11, 7.1 EU GMP Leitfaden Kap. 4
Regelmäßige Sicherungskopien, deren Integrität und Richtigkeit sowie die Datenwiederherstellung ist zu validieren und regelmäßig zu überwachen	EU GMP Annex 11, 7.1
Qualitätssystem des Auftraggebers sollte die Kontrolle und Überprüfung aller ausgelagerten Tätigkeiten einschließen	EU GMP Leitfaden Kap. 7

Tabelle 1: Wichtige Anforderungen aus Gesetzen und Richtlinien

4 QUALIFIZIERUNG UND VALIDIERUNG IN DER CLOUD.

4.1 Grundlagen

Im Rahmen von Cloud Computing sind an Vorgehensweisen und Dokumentation zur Qualifizierung und Validierung an den Cloud Service Provider die gleichen Maßstäbe anzulegen, die für das regulierte Unternehmen gelten.

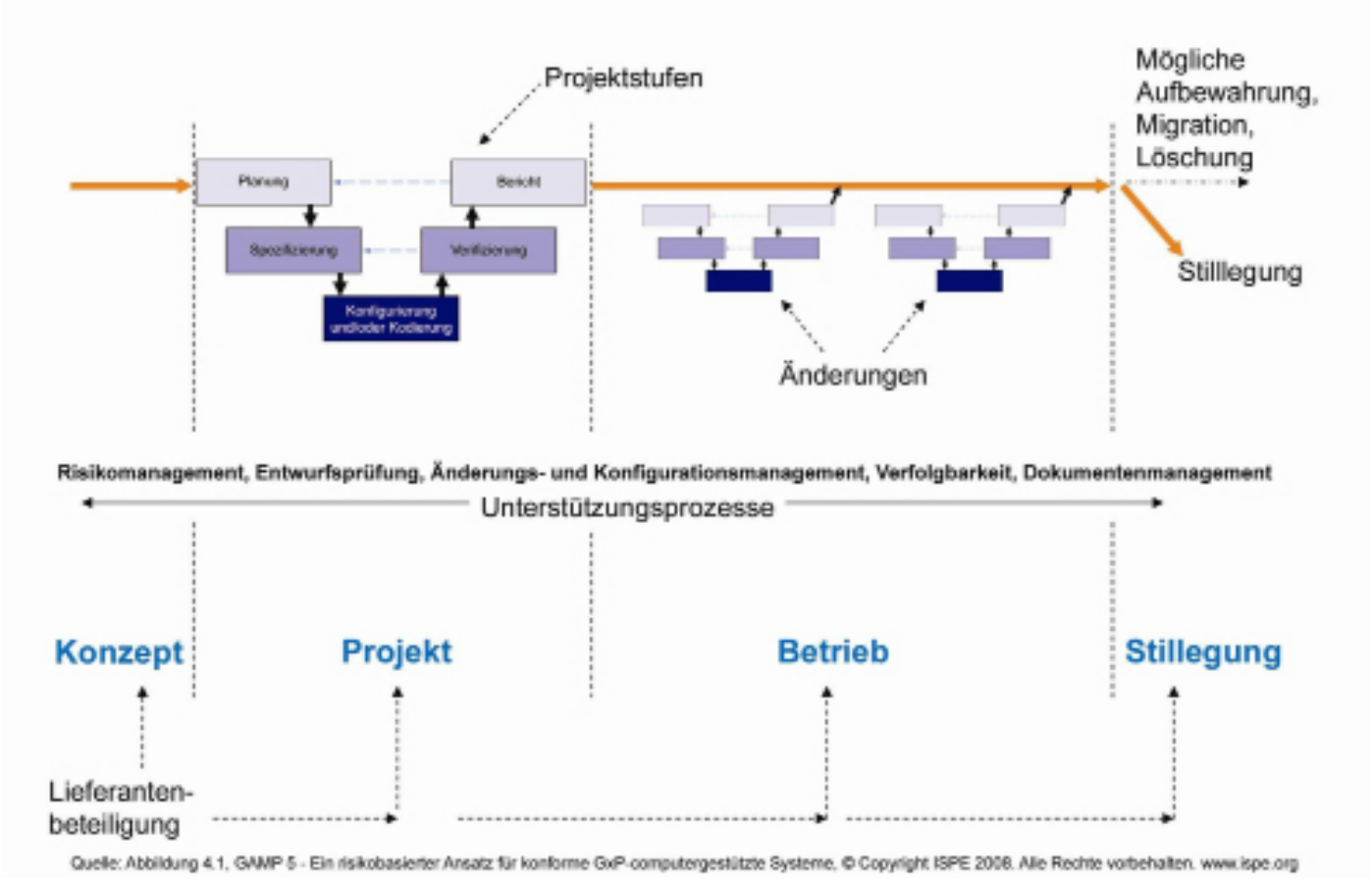


Abbildung 4: Lebenszyklusmodell

So sind sämtliche Aktivitäten – auch im Umfeld der Hardware, der Virtualisierungs- und der Betriebsumgebung – vor einer Umsetzung zu planen und zu spezifizieren.

Die Qualifizierung ist zu dokumentieren und Abweichungen, die im Rahmen der Qualifizierung festgestellt werden, sind risikobasiert zu bewerten und zu dokumentieren. Eine formale Freigabe unter Berücksichtigung ggf. vorhandener Abweichungen für den Betrieb ist zu implementieren.

Das gleiche gilt für den Betrieb. So müssen die Prozesse Change-Management, Incident- und Problem-Management entsprechend um notwendige Freigaben, Informationen und Dokumentationsvorgaben ergänzt werden. Wichtig ist hier die Implementierung eines Risikomanagements in die Prozesse.

4.2 Aufgaben des Cloud Service Providers

Für den Cloud Service Provider bedeutet dies, dass er Prozesse etabliert und in Verfahrensanweisungen niedergelegt hat, die das Vorgehen und die Dokumentation bei der Qualifizierung beschreiben.
Im Fall von „Platform as a Service“ und „Software as a Service“ kommen die Validierungstätigkeiten und deren Beschreibung und Dokumentation hinzu.
Es ist in der Pflicht des Cloud Service Providers, die Prozesse, das Framework von Verfahrensanweisungen und die notwendigen Templates für Dokumente zu erarbeiten. Es ist in der Verantwortung des regulierten Unternehmens, dies im Rahmen von Audits und einem Lieferanten-Management zu überprüfen und zu bewerten.

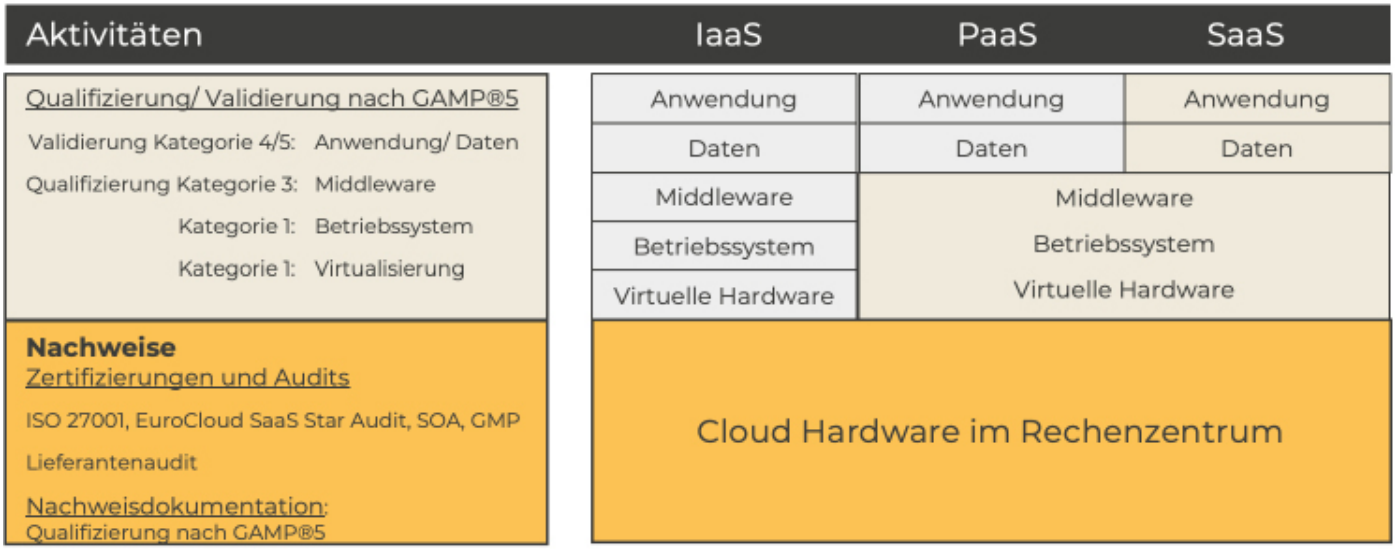


Abbildung 5: Aufgaben des Cloud Service Providers

In Abbildung 5 sind die Aktivitäten des Cloud Service Providers für die Cloud Service-Modelle beschrieben.

Neben den klassischen Zertifizierungen (ISO 9001, ISO 27000, ISO 20000, BSI) ist die Nachweisdokumentation einer Qualifizierung bis zur Middleware zu erbringen (IaaS, PaaS). Wenn der Cloud Service Provider darüber hinaus auch Anwendungen als Dienst zur Verfügung stellt, sind die entsprechenden Validierungsaktivitäten nachzuweisen.

5 WEGE IN DIE CLOUD – AKTIVITÄTEN EINES REGULIERTEN UNTERNEHMENS.

5.1 Konzept- und Design-Phase

Im Rahmen der Konzept- und Design-Phase erfolgt eine Analyse der Applikationen und Daten – und damit der Systeme –, mit denen das regulierte Unternehmen in die Cloud gehen möchte.

Dabei geht es um technische Aspekte der Infrastruktur und das im Unternehmen implementierte Identity Management sowie eine Analyse der Prozesse hinsichtlich der Compliance-Anforderungen. Daraus abgeleitet ist die Beteiligung verschiedener Unternehmensbereiche erforderlich, um eine vollständige und in ihrem Inhalt konsistente Analyse als Entscheidungsgrundlage zu erstellen.

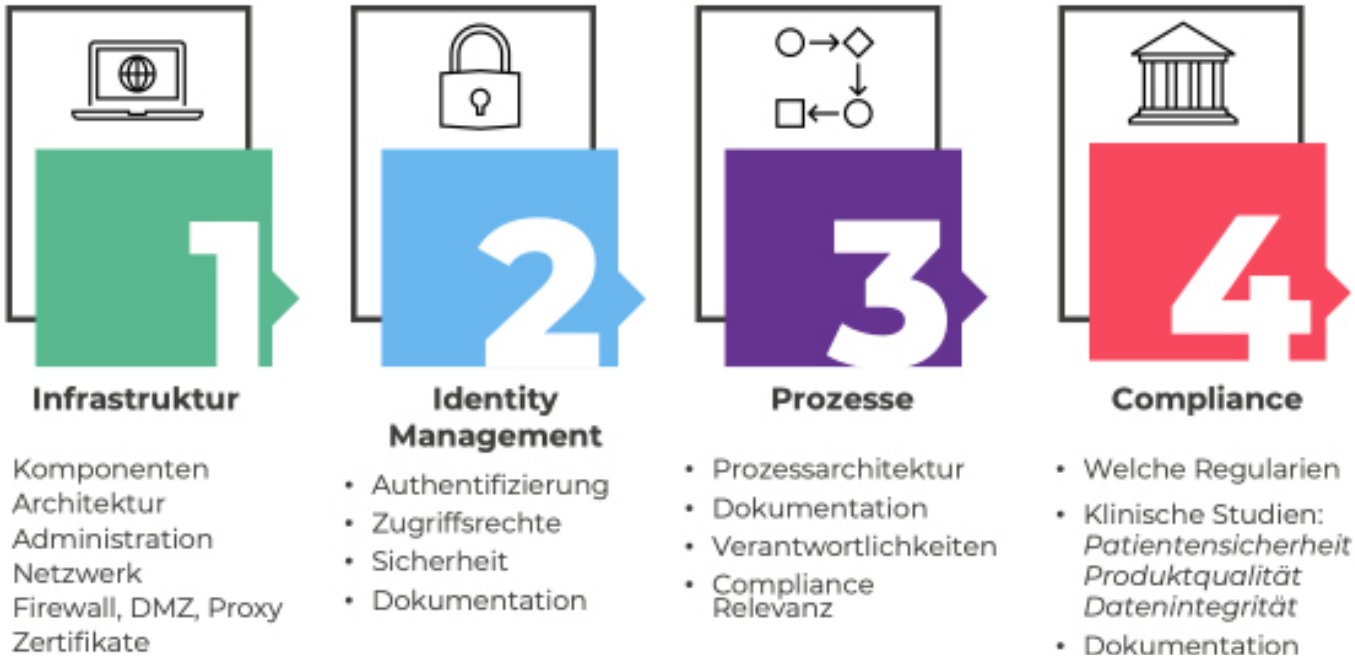


Abbildung 6: Systemanalyse

Für die Durchführung dieser Analyse können zwei Vorgehensmodelle gewählt werden.

5.1.1 Vom Prozess zur Infrastruktur

Beginnend mit der Analyse der Geschäftsprozesse werden diejenigen identifiziert, mit denen man in die Cloud gehen will. Für diese Prozesse wird die Frage nach den für sie geltenden Regulatorischen Anforderungen gestellt und dokumentiert. Dabei geht es um die firmeninternen Vorgaben ebenso wie um gesetzliche Vorschriften aus den Bereichen Finanzen, Datenschutz, Produkthaftung und natürlich um die Aspekte von US FDA/EU GMP.

Daneben sollten in diese Analyse auch die Fragen von Patent- und IP-Themen einfliessen.

In einem zweiten Schritt wird dann geprüft, auf welchen Systemen inkl. der Schnittstellen die Prozesse abgebildet sind. Dabei spielt die Systemarchitektur eine entscheidende Rolle.

In dritten Schritt schliesst sich die Analyse von Zugriffsrechten, Authentifizierungsmechanismen und Fragen der Datensicherheit an.

5.1.2 Vom System zum Prozess

Oft steht die IT-Abteilung vor der Aufgabe, bestimmte Systeme in die Cloud zu migrieren. Hier muss die Analyse von Infrastruktur und den betroffenen Komponenten ausgehen und über die Applikationen der betroffenen Systeme die Zuordnung zu den Prozessen erfolgen.

Anschliessend kann dann eine Einschätzung der Compliance-Vorgaben erfolgen.

5.1.3 Auf die Daten kommt es an

Unabhängig vom Weg, auf dem die Analyse erfolgt: Erst nach einer Betrachtung der Daten, die von der Migration zu einem Cloud Service Provider betroffen sind, können konkrete Aussagen zu Risiken getroffen werden.

Data Classification Assessment ist ein unverzichtbarer Bestandteil bei der Planung einer Migration in die Cloud. Hier geht es um eine Klassifizierung von Daten bezüglich ihres Schutzbedarfs.

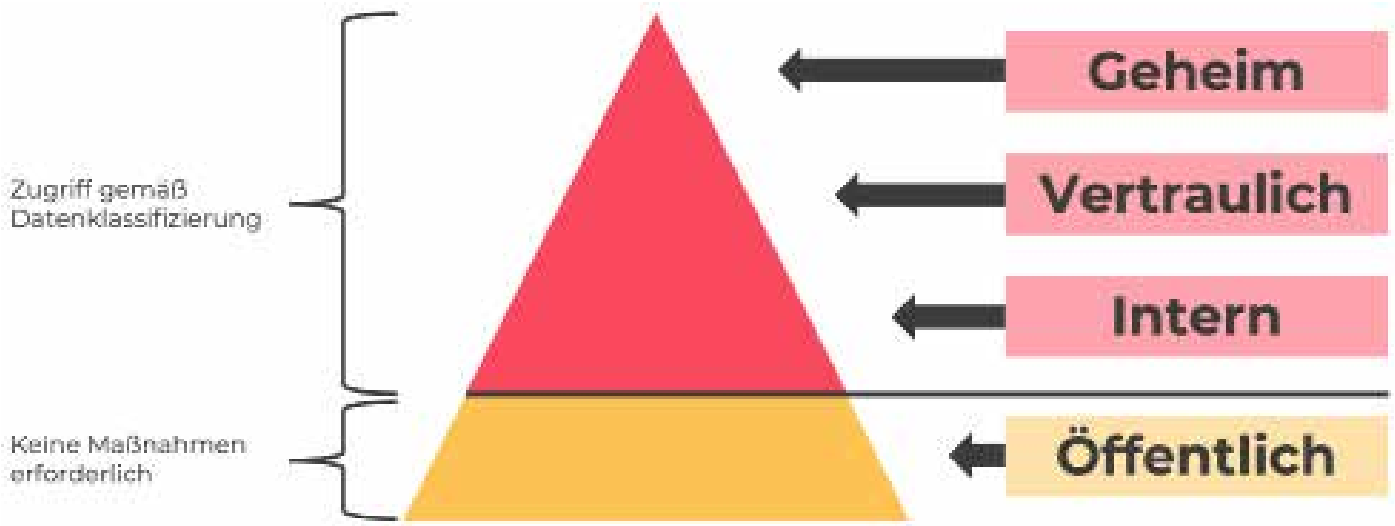


Abbildung 7: Datenklassifizierung

Auf dieser Grundlage ist dann sehr schnell eine Festlegung möglich,mit welchen Daten das Unternehmen in die Cloud gehen kann und mit welchen Maßnahmen ein entsprechender Schutzbedarf in der Cloud sichergestellt werden muss.

5.1.4 IT-Sicherheit und Datenschutz in der Cloud – die Standortfrage

Insbesondere mit Blick auf regulatorisch relevante Daten ist die Frage, wo die Cloud liegt, wo also die Daten tatsächlich gehalten werden, wichtig. Die Systeme und damit auch die auf ihnen verarbeiteten Daten unterliegen im Normalfall den Gesetzen des Landes, in denen sie stehen und betrieben werden. Unterschiedliche Länder haben auch unterschiedliche Standards hinsichtlich Datenschutz.

Das Thema IT-Sicherheit muss im Rahmen der Cloud-Strategie festgelegt werden, bevor geschäftskritische bzw. aus regulatorischer Sicht in besonderem Maße schutzwürdige Daten in die Cloud ausgelagert werden. Grundlage sind die in 5.1.1, 5.1.2 und 5.1.3 beschriebenen Analysen. Ziel muss es sein, frühzeitig mit dem Cloud Service Provider die den Schutzbedarfen entsprechenden Sicherheitsmaßnahmen zu besprechen und festzulegen.

Weitere mittelbar mit dem Thema IT-Sicherheit zusammenhängende Themen betreffen Risiken, die aus dem Einsatz eines Cloud Service Providers als Dienstleister resultieren. So ist die Frage, was bei einer Insolvenz mit den IT-Systemen und damit mit den Daten geschieht, zu stellen. Sind sie Bestandteil der Insolvenzmasse, können sie an andere, vertraglich nicht eingebundene Dritte gehen. Ein unberechtigter Zugriff auf die Daten ist somit nicht auszuschließen. Hier müssen klare vertragliche Regelungen mit dem Cloud Service Provider getroffen werden.

Setzt der Cloud Service Provider selbst Sublieferanten ein, so ist im Rahmen seiner Auditierung ein Fokus auf dessen Vertragsgestaltung und die Kontrolle der Sublieferanten zu legen.

Ein besonderes Augenmerk gilt dem Schutz personenbezogener Daten. Hier spielen der Geschäftssitz und der Standort der Datenverarbeitung eine entscheidende Rolle. Der Gesetzgeber hat in der DSGVO (Datenschutzgrundverordnung) festgelegt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten entweder durch dieses Gesetz, durch andere Rechtsvorschriften erlaubt oder angeordnet werden kann oder der Betroffene eingewilligt hat.

Dieses Verbot mit Erlaubnisvorbehalt ist insbesondere bei der Weitergabe solcher Daten an Dritte zu berücksichtigen. Bedient sich die datenerhebende Stelle – in diesem Falle das Pharma- oder Medizintechnik-Unternehmen – eines Dienstleisters, dann liegt die sog. Auftragsverarbeitung nach Art. 28 DSGVO vor. Eine Auftragsverarbeitung durch z.B. einen Cloud Service Provider bedarf dann nicht der Zustimmung, da es sich in diesem Fall nicht um die Weitergabe von Daten an Dritte handelt. Dies muss jedoch mit dem Cloud Service Provider vertraglich klar geregelt sein.

Ohne hier auf weitere Details der Gesetzgebung eingehen zu wollen, lässt sich jedoch konstatieren: Personenbezogene und besonders schutzwürdige personenbezogene Daten sollten den Rechtsraum der Bundesrepublik Deutschland nicht verlassen.

Anbieter von Cloud Services tragen dem durch das Angebot einer „in country private Cloud“ Rechnung.

5.2 Der Projektplan

Der Projektplan für die Migration von US FDA/EU GMP-relevanten Systemen oder Applikationen sollte anglehnt an die Migrationsplanung, wie sie der GAMP®5 vorschlägt, erfolgen.

Abbildung 8: Migration zum Cloud Service Provider

Die folgenden Schritte sind in den Projektplan aufzunehmen und zu beschreiben:

1. Blick auf die Infrastruktur:
   a) Anwendersicht (Serviceorientierte Anforderungen):
      Applikation und Software, Datenspeicherung und Ablage, Sicherung der Daten, Performance
   b) IT- und Compliance-Sicht
      Zu qualifizierende Infrastrukturkomponenten (spezifizieren, implementieren, konfigurieren, verifizieren)

2. Blick auf die Compliance-Anforderungen:
   a) Welche gesetzlichen Vorgaben und Vorschriften gelten? Diese sind ohne Einschränkung einzuhalten! (das „wie“ ist risikobasiert zu diskutieren)
   b) Gibt es weitere Anforderungen?
      Datenschutz, Business Requirements
   c) Welche Daten dürfen in die Cloud?
   d) Welche Daten dürfen keinesfalls in die Cloud?

3. Mapping der Anforderungen auf mögliche Cloud Services

4. Implementieren der Anforderungen auf den Cloud Service

Die aus dem Projektplan resultierenden Anforderungen an den Cloud Service Provider sind im Rahmen der Lieferantenauswahl zu prüfen.

5.3 Auswahl des Cloud Service Providers / Assessment

Bei der Auswahl des Cloud Service Providers ist der dokumentierte Nachweis zu erbringen, dass alle aus der Analyse der Anforderungen abgeleiteten Vorgaben erfüllt werden können. Dazu ist ein Audit potentieller Cloud Anbieter unerlässlich.

Der Cloud Service Provider muss grundsätzlich nachweisen, dass er auf der Grundlage der technischen und physikalischen Sicherheit (Zugangsschutz, Gebäudearchitektur, Redundanz der Versorgungskomponenten, Brandschutz, Schutz vor Elementarschäden) die Vertraulichkeit, Integrität und Verfügbarkeit der Daten realisieren kann.

Weiterhin ist der Nachweis der Mandantenfähigkeit auf allen Ebenen des Cloud Computing Stacks zu erbringen. Ein Information Security Management System (ISMS) seitens des Cloud Providers ist unerlässlich. Der Nachweis kann über entsprechende Zertifikate (z.B. ISO 27001, SAS) erfolgen. Ein Zertifikat ersetzt jedoch nicht ein Audit vor Ort, bei dem man insbesondere die technische und physikalische Sicherheit in Augenschein nehmen kann.

Der Nachweis einer Compliance, z.B. mit dem Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), dem Payment Card Industry (PCI) Standard oder mit US FDA /EU GMP, kann durch Auditberichte, die der Cloud Service Provider vorlegt, besser aber durch ein selbst durchgeführtes Audit belegt werden.

Darüber hinaus muss der Cloud Service Provider den Nachweis erbringen, dass er über ein dokumentiertes Framework von Prozessen verfügt, seine Systeme qualifiziert (im Sinne von US FDA und EU GMP) zu implementieren und zu betreiben. Insbesondere die Frage nach der Sicherstellung der Standortzusagen für Daten und Applikationen ist zu verifizieren.

Hierzu ist ein entsprechender Fragenkatalog [5] hilfreich, der die notwendigen Anforderungen beinhaltet und eine Bewertung der verschiedenen Provider ermöglicht. Das Ergebnis deses Audits ist im Sinne eines GMP-Lieferantenaudits zu dokumentieren und in ein Lieferanten-management zu überführen.

6 AUFGABEN DES CLOUD SERVICE PROVIDERS.

Zu den Aufgaben des Cloud Service Providers gehört neben der Mitwirkung bei der Auditierung auch die Gewährleistung der Integration von Qualifzierungs- und Validierungsaufgaben in das Projekt Management.

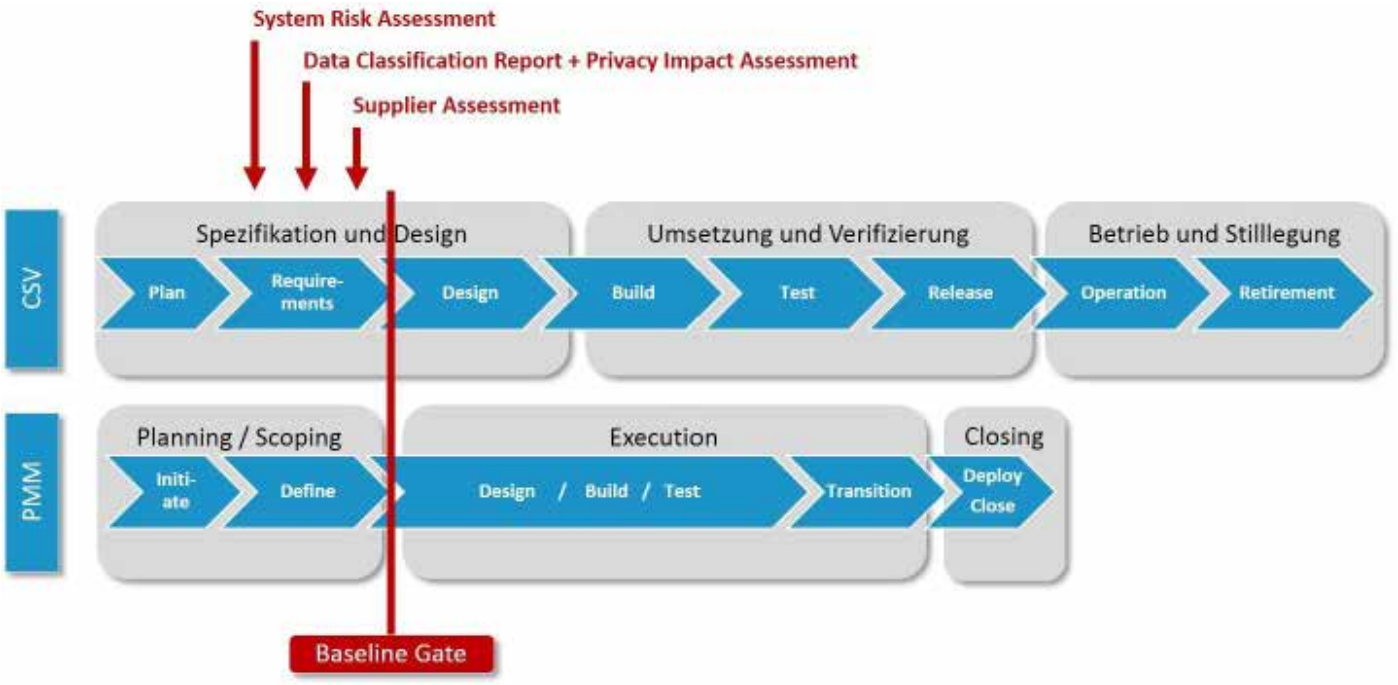


Abbildung 9: Projektmanagement (PMM) und Qualifizierung (CSV)

Der Cloud Service Provider muss über Verfahrensanweisungen für GMP-konforme Implementierung und Betrieb von Infrastruktur-Komponenten verfügen, in denen die provider-spezifische Vorgehensweise beschrieben wird. Weiterhin sollten Templates oder Tools zur Unterstützung dieser Prozesse vorhanden sein.

Da dies von Provider zu Provider unterschiedlich umgesetzt sein kann, müssen die folgenden Mindestanforderungen erfüllt sein:

- IT-Prozesse müssen den GMP-Anforderungen Rechnung tragen (Sicherstellung, dass ein System keinen ungeplanten Änderungen ausgesetzt ist)
  - Change Management
  - Incident Management
  - Problem Management

- Ein Schulungskonzept unter Berücksichtigung der GMP-Anforderungen muss etabliert und dokumentiert sein
- Vorgaben zu Qualifizierung und Validierung (im Fall von SaaS) müssen Planung, Verifizierung und Freigaben beinhalten, diesbezügliche Rollen müssen von qualifiziertem Personal ausgefüllt werden
    - Template-basiert
    - Toolbasiert

So zeichnet der Cloud Service Provider grundsätzlich für die in der folgenden Tabelle dargestellten Dokumente eines Qualifizierungs- und Validierungsframeworks verantwortlich.

Dokument	Software a a Service	Platform as a Service	Infrastructure as a Service
Validation Plan / Qualification Plan	X	X	X
User Requirement Specification	X		
Functional Specification	X	X	
Design Specification	X	X	
Installation Specification	X	X	X
Operational Specification	X	X	
Performance Specification	X		
Validation Report / Qualification report	X	X	X

Tabelle 2: Dokumenten Matrix

Der Cloud Service Provider muss für IT-Prozesse, in denen nach GMP-Vorgaben Prozessowner in die Entscheidungen einzubeziehen sind, entsprechende Schnittstellen zum regulierten Unternehmen definieren.

Der Cloud Service Provider muss sich einer regelmäßigen Überprüfung seiner Aktivitäten durch das regulierte Unternehmen in Form von Audits unterziehen.

Der Cloud Service Provider muss sich mit den aus den Audits resultierenden kritischen Abweichungen zwingend auseinandersetzen. Im Fall nichtkritischer Abweichungen obliegt es der Abstimmung zwischen dem regulierten Unternehmen und dem Cloud Service Provider, ein Vorgehen zu definieren.

Der Cloud Service Provider muss dem regulierten Unternehmen zuvor vertraglich festgelegte Reports zur Verfügung stellen.

Der Cloud Service Provider ist verpflichtet, alle Abweichungen und unerwarteten Ereignisse die Systeme des regulierten Unternehmens betreffend sofort an dieses weiter zu geben.

Im Rahmen seiner Prozesse muss sichergestellt und durch das regulierte Unternehmen regelmäßig geprüft werden, dass

- Daten entlang der Aufbewahrungsfrist (definiert vom regulierten Unternehmen) verfügbar sind,
- der Zugriff auf Daten für einen unverzüglichen Rückruf schnell möglich ist,
- die gespeicherten Daten gegen Verlust und Beschädigung geschützt sind,
- ein Zugriff auf Daten auf befugte Personen beschränkt ist,
- formale Vereinbarungen zur Regelung von Verantwortlichkeiten von Lieferanten und Dienstleistern existieren,
- ein Nachweis der Kompetenz und Zuverlässigkeit des Lieferanten durch regelmäßige Audits und Überprüfungen erbracht wird,
- Informationen zu Qualitätssystem und Audits den Behörden auf Nachfrage jederzeit zur Verfügung gestellt werden können,
- Verfügbarkeit, Lesbarkeit und Richtigkeit gespeicherter Daten regelmäßig überprüft wird,
- Regelmäßige Sicherungskopien, deren Integrität und Richtigkeit sowie die Datenwiederherstellung validiert und regelmäßig überwacht wird und
- das Qualitätssystem des regulierten Unternehmens die Kontrolle und die Überprüfung aller ausgelagerten Tätigkeiten einschließt.

7 ZUSAMMENFASSUNG.

Die sorgfältige Analyse zu Cloud Service-Modell, Daten, Prozessen und Applikationen sowie der Infrastruktur ermöglicht es:

1. eine Cloud-Strategie zu entwickeln,
2. einen Projektplan für die Migration in die Cloud aufzustellen,
3. die Auswahlkriterien für den Cloud Service Provider festzulegen und die entsprechenden Audits zu planen,
4. eine Migrations-Lifecycle-Dokumentation für eine FDA-/GMP-konforme Migration festzulegen,
5. die Vertragsgestaltung mit dem Cloud Service Provider festzulegen und
6. geeignete Kontrollen für die Aufrechterhaltung der behördlichen Konformität zu definieren.

Für die Umsetzung einer erfolgreichen Migration zu einem Cloud Service Provider mit US FDA/EU GMP-relevanten Applikationen und Systemen sind neben technischen Kenntnissen zu den Cloud-Diensten und der Migration umfangreiches Prozess-Know-how und regulatorisches Wissen notwendig.

Wir beraten Sie gerne bei der Analyse Ihrer Systeme, der Auswahl von richtiger Strategie und Konzept für Ihr Cloud Computing sowie bei der Entscheidung für den richtigen Provider.

8 LITERATUR.

[1] e-Daten- und Dokumentenmanagement in der Klinischen Forschung, Qualitätssicherung bei elektronischen Systemen
Dr. Andreas Jabs, Klaus Völlmecke, pharmind – Die Pharmazeutische Industrie, 05/2013

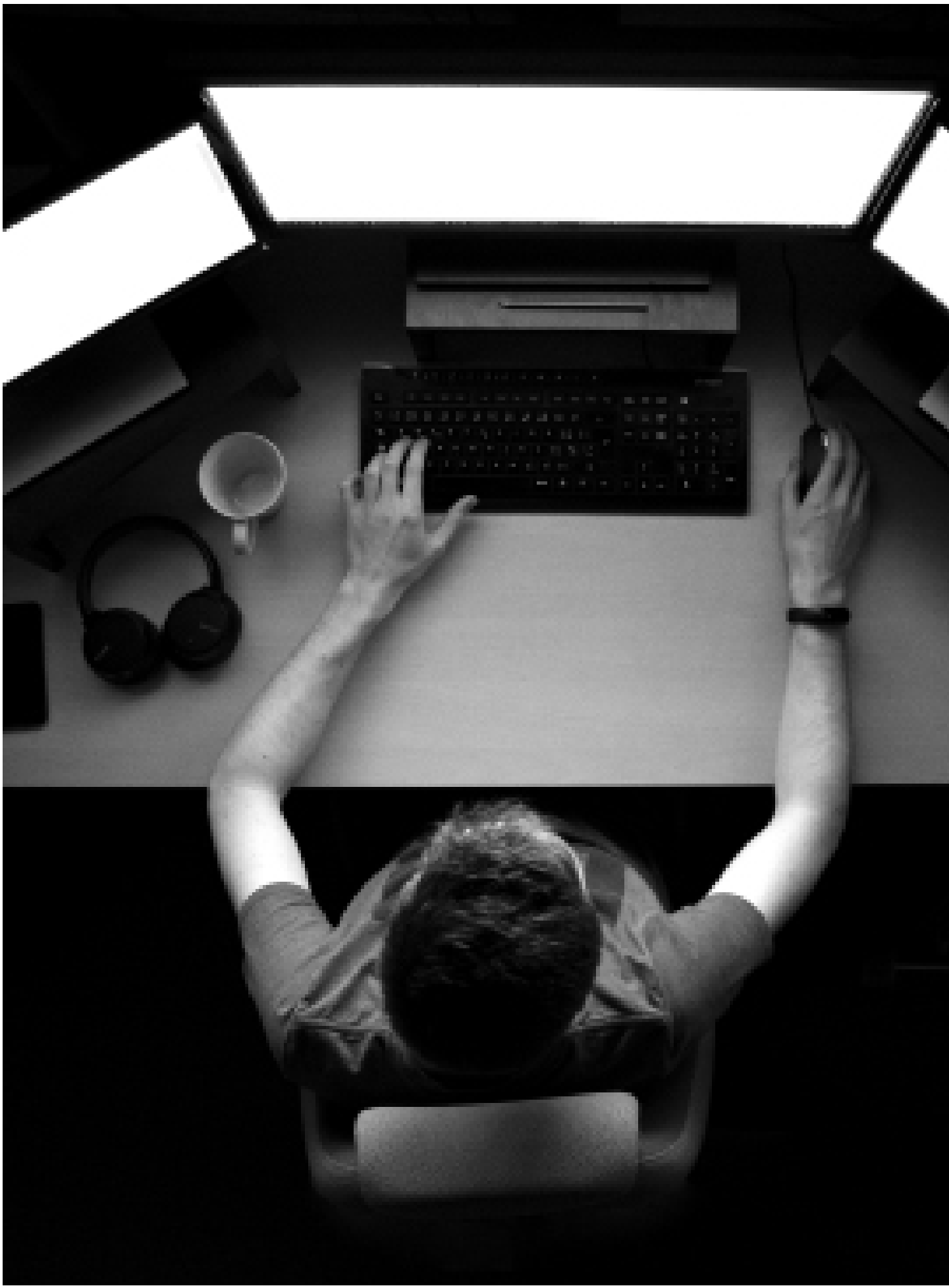
[2] XCLINICAL – Clinical Trial Software from A to X, XClincial GmbH München, xclinical.com

[3] MedSurv – das individualisierbare Internetportal für klinische Studien der Phase I-IV, www.medsurv.de

[4] EU GMP Annex 11 „Computerised Systems“

[5] Devoteam Alegri Assessment Data Center

9 ABBILDUNGEN UND TABELLEN.



ÜBER DEVOTEAM

Bei Devoteam bieten wir innovative Technologieberatung für Unternehmen. Als reiner Player der digitalen Transformation für führende Organisationen in ganz EMEA sind unsere 8000 Profis bestrebt, sicherzustellen, dass unsere Kunden ihre digitalen Schlachten gewinnen. Mit einer einzigartigen Transformations-DNA verbinden wir Business und Technologie.

Wir sind in 18 Ländern in Europa und im Nahen Osten präsent und zeichnen auf mehr als 25 Jahre Erfahrung zurück und gestalten Technologie für Menschen, so dass sie Mehrwert für unsere Kunden, für unsere Partner und für unsere Mitarbeiter schafft.

Creative tech for Better Change.

ÜBER M CLOUD

Mit 500+ Kunden ist Devoteam M Cloud einer der weltweit führenden Anbieter von Microsoft Cloud-Technologien mit derzeit 16 Goldzertifizierungen und 2 Advanced Spezializations - “Kubernetes on Microsoft Azure” und “Adoption and Change Management”. Unsere 800+ Microsoft Experten in EMEA bieten mittelständischen und großen Unternehmen ein Lösungs- und Produktportfolio an, das die Digitalisierung und neue Formen der Zusammenarbeit ermöglicht sowie eine gründliche Analyse von Unternehmens- und Produktionsdaten zur Realität werden lässt. Devoteam M Cloud modernisiert Ihre gesamte IT-Architektur, begleitet Sie auf ihrem Weg in die Cloud und macht Sie fit für die digitale Zukunft.

Fakten:

500+ Kunden

1300+ Zertifikationen und 800+ Microsoft Experten in EMEA

16 Gold Zertifikationen und 2 Advanced Specializations

Microsoft Gold Partner

Microsoft | Multi Area Partner Orchestration

Microsoft in Education Global Training Partner

devoteam M Cloud

KONTAKT: DE.DEVOTEAM.COM/KONTAKT/

devoteam
M Cloud

Creative tech for Better Change