



## UNSER DIENSTLEISTUNGSANGEBOT ENTLANG DES CLOUD LIFE CYCLES

---

In&Out AG

Erfahrungsbericht aus fünf erfolgreichen Projekten

Datum: 06.10.2021

---

## CLOUD STRATEGIE

**Logicare AG** ist ein von Spitälern gegründetes und auf IT-Dienstleistungen spezialisiertes Unternehmen, welches umfassende Lösungen für Akutspitäler und weitere Institutionen des Gesundheitswesens konzipiert und realisiert. Als zentraler Ansprechpartner rund um die digitale Transformation im Gesundheitswesen bündelt Logicare vielfältige Kompetenzen und umfassende Angebote.

Wie in den meisten IT Organisationen besteht auch bei der Logicare ein Kostendruck und Sparpotentiale müssen geortet und wenn möglich ausgenutzt werden. In diesem Rahmen stehen auch Überlegungen zu «make or buy». Um sich in diesem Kontext richtig zu positionieren und um die eigene Cloud Readiness zu erhöhen, wurde In&Out beauftragt, eine entsprechende *Cloud Strategie* auszuarbeiten.

### ANALYSE SERVICES UND HANDLUNGSBEDARF

Mit einer Risikoanalyse wurde zu Beginn der Arbeiten die Situation bezüglich des eigenen Angebots, der Nachfrage und der Konkurrenz aber auch der kritischen Erfolgsfaktoren erhoben. Dabei hat sich gezeigt, dass die angebotenen Services weiterhin gefragt sind, aber auch, dass Potential sowohl beim Angebot wie auch bei der Service-Bereitstellung besteht. Weiter muss der Tatsache des Preiserfalls bei IT Hardware Rechnung getragen werden.

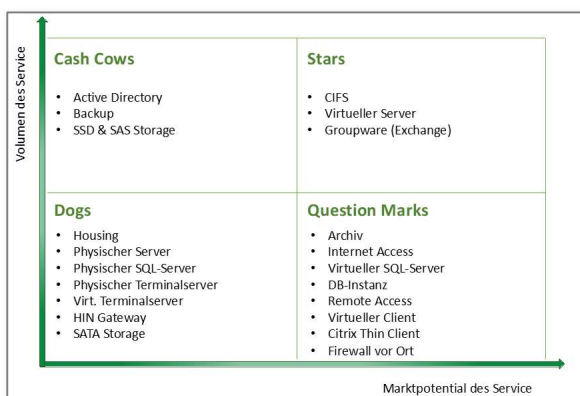


Abbildung 1 – LGC Services nach Boston Consulting Group

Bezüglich der Cloud Readiness kann festgehalten werden, dass Software-Hersteller und -Lieferanten im Healthcare-Umfeld zum Zeitpunkt der Analyse ihre Applikationen noch wenig Cloud-fähig anbieten. Der Fokus im Gesundheitswesen lag primär bei der Digitalisierung von Dokumenten und Prozessen, dem Nutzen von Standardlösungen sowie

der Einführung des elektronischen Patientendossiers (EPD).

Die Erhebungen haben aber auch aufgezeigt, dass direkte Mitbewerber bereits Cloud-Lösungen anbieten oder Ihre Kunden betreffend einer Cloud-Adoption unterstützen können. Logicare will hier zukünftig führend am Markt sein und die notwendigen Schritte einleiten.

Aktuelle Trend Analysen weisen auch im Gesundheitswesen auf eine grosse Digitalisierungswelle hin. Um hier Kunden zukunftsweisend unterstützen zu können, ist ein fundiertes Cloud Know-how und ein entsprechendes Service-Angebot für Service Provider notwendig.

### POTENTIAL DER CLOUD SOURCING MODELLE

Über Kriterien wie Flexibilität, Skalierbarkeit oder Sicherstellung der Security & Compliance Anforderungen wurden im Rahmen der Arbeiten mit einer *Potentialanalyse* die drei Sourcing Modelle

- OnPrem – aktuelles Betriebsmodell, kann als Variante den Aufbau eines eigenen Cloud-Stacks beinhalten
- Hybrid Cloud Modell – Mischform von Private Cloud und Public Cloud (Private Cloud mit zwei Ausprägungen möglich: OnPrem oder bei Provider eingekauft)
- Multi Cloud Modell – reine Public Cloud Lösung mit verschiedenen Providern

im Detail betrachtet und der Nutzen für Logicare beurteilt.

### NUTZEN UND EMPFEHLUNGEN

Mit dem Wissen aus den durchgeführten Analysen wurde für die Logicare eine Cloud Strategie ausgearbeitet. Diese Strategie basiert auf einer **Hybrid Cloud**. Mit dieser Lösung kann gewährleistet werden, dass sensitive Gesundheitsdaten ausschliesslich in der Schweiz gespeichert und bearbeitet werden, aber auch, dass das grosse Potential der Public Cloud genutzt wird. Mit der Hybrid Cloud wird das Service Angebot der Logicare **innovativ, flexibel und skalierbar** – Stichworte dazu sind Pay-as-you-use und Best-of-Breed-Approach. Wichtige und wertvolle Cloud Erfahrungen für den späteren Bezug von Cloud Health-Care Services, bspw. Datenanalysen oder KI, können mit der Umsetzung dieser Strategie gemacht werden.

## PRÜFUNG DER CLOUD READINESS

Die **Media Firma** ist in der Vermarktung von Sportveranstaltungen tätig. Dabei werden unter anderem Sportwerbung (Bandenwerbung, etc.) und zum Teil Fernsehübertragungen für Sportveranstaltungen produziert.

Die für den operativen Betrieb benötigte IT wird in Zug vollständig OnPremise bereitgestellt. Über Remote Desktop wird weltweit auf Programme und Daten zugegriffen. Mit Hilfe des **In&Out Cloud Transition Service CTS** wollte die Media Firma eine Auslegeordnung der IT Services bezüglich deren Cloud Readiness erhalten. Dabei soll aufgezeigt werden, welche Services sich zukünftig für einen Betrieb in der Cloud eignen. Der Einsatz von SaaS soll gegenüber IaaS und PaaS im Vordergrund stehen.

## PRÜFUNG DER CLOUD READINESS

Um ein gemeinsames Verständnis zu erlangen, sieht der Prüfprozess vor, dass zu Beginn wichtige Funktionen und Begriffe der Cloud Technologie abgestimmt werden.

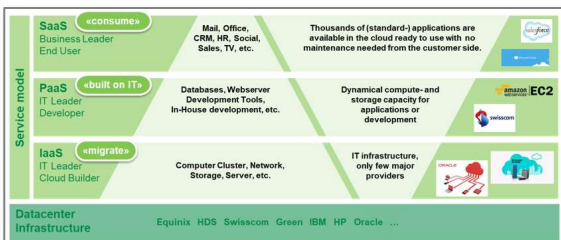


Abbildung 2 – Cloud Service Model Terminologie

Entlang der Strategie «SaaS before PaaS before IaaS» wurden mit Hilfe des standardisierten CTS Fragebogens sämtliche relevanten Applikationen zusammen mit den Spezialisten der Media Firma analysiert. Besprochen werden dabei unter anderem vorhandene IT Architekturen & Infrastrukturen, Betriebsprozesse, Security Massnahmen sowie die IT Strategie und Business Funktionalitäten.

Bei den Erhebungen wurden Fragen wie zum Beispiel die folgenden beantwortet:

- Wie passt der Service (oder die Applikation) zur IT Strategie?
- Wie ist der Schutzbedarf des Service definiert?
- Wie werden Benutzer und Berechtigungen verwaltet?
- Kann der Service vollständig auf einer virtualisierten Infrastruktur betrieben werden?

- Sind die Betriebskosten des Service bekannt? Pro Applikation sind insgesamt rund 20 Fragen zu beantworten.

## ERGEBNISSE DER ANALYSE

Die Analyse mit CTS geschieht über Interviews und Stichprobenprüfung. Fragen und mögliche Antworten sind vorbereitet. Die Bewertungskriterien sind, ähnlich einer Nutzwertanalyse, gewichtet. Diese Gewichtung wurde zu Beginn des Analyse-Prozesses mit der Media Firma erstellt.

Verschiedene Graphiken und Visualisierungen fassen die Ergebnisse zusammen und machen sie damit gut verständlich. Die folgenden zwei Beispiele an Visualisierungen unterstreichen dies.

In&Out AG - Cloud Transition Service							
Bewertungs-Übersicht Services / Applikationen / Anwendungen (S/A)							
Großfilter							
Name Service / Applikation	Funktion	Gewichtete Bewertung pro Kategorie					Gesamtbewertung
		Strategie / GRC	IT-Sicherheit	Business	Infrastruktur	Betrieb	
App A	Manuelle Performance Management	Überprüfung notwendig	Einfache Transition	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig
App B	Business Performance-Management-König	Überprüfung notwendig	Abwägend notwendig	Überprüfung notwendig	Überprüfung notwendig	Einfache Transition	Überprüfung notwendig
App C	Buchhaltung	Überprüfung notwendig	Einfache Transition	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig
App D	CRM	Überprüfung notwendig	Überprüfung notwendig	Einfache Transition	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig
App E	Contract Mgmt and Order Abgabe für non-business Verträge	Überprüfung notwendig	Überprüfung notwendig	Einfache Transition	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig
App F	Payroll CI	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig	Überprüfung notwendig	Einfache Transition	Überprüfung notwendig
App G	E-Mail Server	Überprüfung notwendig	Abwägend notwendig	Überprüfung notwendig	Einfache Transition	Überprüfung notwendig	Überprüfung notwendig
App H	E-Mail Archiv	Überprüfung notwendig	Einfache Transition	Einfache Transition	Einfache Transition	Überprüfung notwendig	Überprüfung notwendig

Abbildung 3 – Heat Map (Werte exemplarisch)

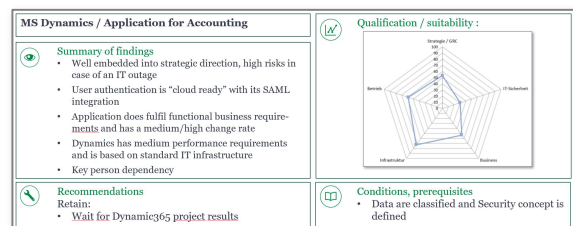


Abbildung 4 – Zusammenfassung der Resultate pro Service

## NUTZEN UND EMPFEHLUNGEN

Die Erhebung bei der Media Firma hat ein **gutes Potential** für den Einsatz von Cloud Services gezeigt. Verschiedene Services sind ohne grosse Aufwände in einem Cloud Environment zu betreiben. Dieses Potential wurde im Rahmen des Auftrags (Fixpreis) in einer Power Point Präsentation aufbereitet und dem IT Management vorgestellt. Dabei wurden pro analysiertem Service eine Empfehlung zum weiteren Vorgehen abgegeben und damit der Grundstein für die weiteren Schritte auf dem Weg in die Cloud gelegt.

## CLOUD RISK ASSESSMENT

Die **Versicherung A** ist eine der ältesten Versicherungsgesellschaft der Schweiz. Sie hat eine Cloud Strategie erarbeitet und im Zuge dieser Strategie erste Cloud Services (IaaS, PaaS und SaaS) in die bestehende IT Landschaft integriert. In einem weiteren Schritt evaluierte die Versicherung A einen spezialisierten Hyperscaler als möglichen Preferred Public Cloud Provider. Als Voraussetzung einer solchen Zusammenarbeit definierte die Versicherung unter anderem die Durchführung einer Risikoanalyse RA, welche die Erfüllung der eigenen Sicherheitsanforderungen überprüft. In&Out wurde mit der Durchführung dieser Risikoanalyse beauftragt.

### RISIKOANALYSE

Die erarbeitete Risikoanalyse gliedert sich in die folgenden Abschnitte:

- *Systembeschreibung* mit der Dokumentation zur Integration resp. zum Aufbau der relevanten Schutzobjekte
- *Schwachstellenanalyse* aufgebaut auf der Systembeschreibung mit einer Auflistung von Massnahmen
- *Sicherheitsmassnahmen* mit einer Beschreibung der abgeleiteten und empfohlenen Massnahmen zum Betrieb einer sicheren Provider Cloud Infrastruktur.

### Grundlagen

Gruppiert nach Datenbeständen, Benutzergruppen, Anwendungsfälle wurden insgesamt 22 Schutzobjekte definiert. Hinzu kommen 24 verschiedene Schadenszenarien. Diese Parameter werden zur Erhebung der Risiken referenziert.

### Analyse

Relevante Risiken entstehen dort, wo eine allgemeine Bedrohung (z.B. Schadsoftware, Trojaner und Viren) auf Grund einer Schwachstelle zu einem Schadenszenario führen kann. Schwachstellen stehen typischerweise im Zusammenhang mit einem Anwendungsfall, weshalb die Risikoanalyse entlang dieser Schutzobjekte erfolgt.

Die Tragweite leitet sich jeweils aus den Schadenszenarien ab. Die Eintretenswahrscheinlichkeit muss auf Grund von Erfahrungswerten und Expertenwissen geschätzt werden und ist mit einer gewissen Unschärfe behaftet.

		Schadensausmass				
		≤ 50k	≤ 250k	≤ 1 Mio	≤ 5 Mio	>5 Mio
Frequenz	< Wöchentlich					
	Monatlich		14-1			
	Quartalsweise		1-1 / 3-1	11-1		
	Jährlich		8-1	1-2 / 2-1 / 2-2 2-3 / 9-1	5-1 / 10-1 / 12-1	
	> Jährlich				6-1 / 13-1 / 13-2	4-1 / 7-1 / 13-3

Abbildung 5 - Risikobeurteilung

Insgesamt wurden 19 Risiken adressiert, wobei kein einziges in der Stufe «hoch» (roter Bereich).

### DIE WICHTIGSTEN ERKENNTNISSE

Die im Rahmen der Risikoanalyse gewonnenen Erkenntnisse waren positiv. Sicherheitsmerkmale wie die Folgenden werden durch den Provider erfüllt und sind bei jeder Cloud Integration zu beachten:

- Detaillierte Dokumentation der Services und deren Integration
- Sicherheitsfunktionalitäten nach heutigem Industriestandard wie zum Beispiel
  - Gut integrierte, moderne und strukturierte Benutzer- und Berechtigungsverwaltung
  - Funktionen für Datenverschlüsselung In Transit und At Rest inkl. Key Management
- Komplette Infrastruktur für das Logging und Monitoring
- Gut strukturierte Verfügbarkeitslevel mit verschiedenen Zonen an geographisch getrennten Standorten
- Alle wichtigen ISO Zertifizierungen vorhanden
- Regelmässige Überprüfung der Installationen, Sicherheitsmassnahmen und Prozesse durch externe Spezialisten
- Garantierte Erfüllung der EU-DSGVO/GDPR Datenschutzrichtlinien.

### NUTZEN UND EMPFEHLUNGEN

Die Versicherung A weiss nun, dass der überprüfte Hyperscaler seine Cloud Services nach dem heutigen Stand der Technik betreibt. Es besteht ein **vollständiges Set an Sicherheitservices** welches in die bestehende Sicherheitsinfrastruktur der Versicherung A integriert werden kann. Die notwendigen Sicherheitsmassnahmen, referenziert auf die eruierten Risiken, sind beschrieben. Die eigenen **Sicherheitsanforderungen können damit erfüllt werden** und einer Nutzung der analysierten Cloud-Services steht nichts im Weg.



## PRIVATE CLOUD PROVIDER EVALUATION UND EINFÜHRUNG

Bei der **Swiss Life** handelt es sich ebenfalls um eine Versicherung, welche als Spezialistin für Finanzplanung und Altersvorsorge am Markt auftritt. Die Swiss Life hat eine IT und Cloud Strategie definiert und dabei festgelegt, dass die bestehenden Data Center DC vollständig aufgelöst und sämtliche IT Services in einer Hybrid Cloud produziert werden sollen. Diese Journey to the Cloud durfte In&Out als externe Projektleiterin umsetzen.

### ANFORDERUNGEN UND EVALUATION

Basierend auf einem vorgängig durchgeführten RfI wurde der Prozess mit einem Request for Proposal RfP gestartet. Dazu wurde ein umfangreicher Frage- und Kriterienkatalog in den Themenkreisen *Provider/Firma*, *Operations* und *Technik* mit insgesamt rund 290 Positionen erarbeitet. Zusammen mit der Beschreibung der angestrebten Ziellösung im RfP Dokument wurde das Dossier an drei, über den RfI vorevaluierte Cloud Provider versendet. Eines der Hauptkriterien für die Private Cloud Ziel-Lösung war die Nutzung von Microsoft Azure als Cloud Stack. Mit dieser Anforderung wird eine vereinfachte Integration der MS Azure Public Cloud in den Hybrid Set-up erreicht. Die Evaluation des Providers erfolgte über die Schritte *Auswertung Angebote*, *Präsentation der Angebote*, *Nutzwertanalyse* und *Due Diligence* (Prozess, Technik und Finanzen). Mit der Nutzwertanalyse wurden die Angebote im Detail zueinander verglichen.

Kriterium	1	2	3
Cloud Allgemein	3	2,2	2,5
Servicezeiten	3	2,2	2,5
Flexibilität	3	2,2	2,5
... (and many more rows) ...			
<b>Zusammenfassung</b>	<b>2,5</b>	<b>2,3</b>	<b>3,2</b>

Abbildung 6 – Ausschnitt Nutzwertanalyse

Aus den Resultaten der Nutzwertanalyse ergab sich eine Rangliste, welche im vorliegenden Fall einen klaren Sieger hervorbrachte. Über einen Business Case, welcher den bestehenden Data Center Set-up mit der zukünftigen Hybrid

Cloud verglichen, wurde ein Pay Back von 3.4 Jahren errechnet.

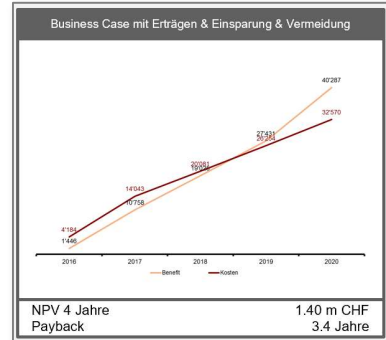


Abbildung 7 – Business Case

Zusammen mit den ebenfalls guten Resultaten aus der Due Diligence, konnte der Auftrag an den Sieger der Evaluation vergeben werden.

### INTEGRATION

In einem ersten Schritt der Phase Integration wurde ein Proof of Concept durchgeführt und die daraus gewonnen Erkenntnisse flossen direkt in die Ziel-Architektur ein.

Um auch ältere Applikationen in der Private Cloud betreiben zu können, wurden zwei Zonen aufgebaut – «Cloud Ready» und «Legacy». Cloud Ready Applikationen müssen entsprechende Anforderungen wie z.B. die User Authentifizierung mit SAML erfüllen wohingegen Legacy Applikationen zentrale Service Accounts nutzen können. Die wesentlichen Herausforderungen bei der Integration waren

- Systemstabilität, welche durch den Einsatz von neuesten, zum Teil noch nicht ausgereiften Technologien negativ beeinflusst wurde
- Hoher Termin Druck, hervorgerufen durch vertragliche Abhängigkeiten bei den bestehenden DC
- Hoher Personal-Ressourcen Bedarf

Insgesamt wurden 1'057 VM, 273 Applikationen und 793 TB Daten in die Hybrid Cloud migriert.

### NUTZEN

Die Swiss Life hat nach 21 Monaten Projektarbeit für Aufbau und Migration die angestrebten **Ziele mit einer georedundanten und ausfallsicheren Privat Cloud vollumfänglich erreicht** und konnte die bestehenden DC termingerecht deaktivieren.

## PUBLIC CLOUD ITSCM-STRATEGIE

Die **Versicherung B** gehört zu den grössten Versicherungen der Schweiz. Sie hat eine Cloud-Strategie erarbeitet mit dem Ziel, in den nächsten 3 - 4 Jahren den grössten Teil der IT-Services aus den eigenen Data Center DC zu Microsoft Azure zu migrieren. Nicht cloud-fähige IT-Services sollen bei einem spezialisierten Provider untergebracht werden und die eigenen DC danach vollständig geschlossen werden.

In diesem Kontext sind Lösungen für das IT Service Continuity Management ITSCM zentral.

### ANFORDERUNGEN UND EVALUATION

#### Anforderungen

Bei den Anforderungen standen folgende Punkte im Fokus:

- Minimierung der Risiken
- Technische Umsetzbarkeit
- «Einfache» Betreibbarkeit
- «Einfache» Testbarkeit (DR-Test)
- Tiefe Kosten
- Alles in der Schweiz

#### Varianten

Basierend auf den Anforderungen wurden in einem ersten Schritt verschiedene Varianten ausgearbeitet. Berücksichtigt wurde dabei die beiden bestehenden Azure Regionen CH North und West sowie die Ankündigung von Microsoft, dass die Region CH North noch im Jahr 2021 auf 3 Verfügbarkeitszonen ausgebaut werden soll.

Folgende drei Hauptvarianten wurden definiert:

- DR aus der Region CH North in die Region CH West

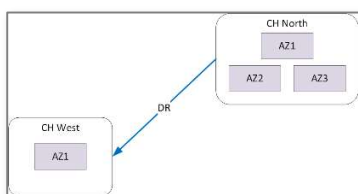


Abbildung 8 - DR Variante 1

- DR innerhalb der Region CH North über die Verfügbarkeitszonen hinweg

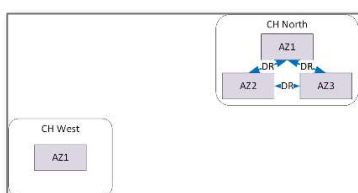


Abbildung 9 - DR Variante 2

- DR innerhalb der Region CH North über die Verfügbarkeitszonen hinweg mit einer zusätzlichen Backupkopie in die Region CH West

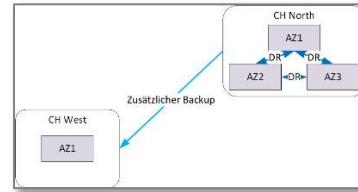


Abbildung 10 - DR Variante 3

In einem zweiten Schritt wurden die wichtigsten Azure-Services wie z.B. VMs, SQL DBs / Managed Instances und Storage Accounts auf deren Umsetzbarkeit, Betreibbarkeit, Testbarkeit und Kosten pro Variante überprüft.

#### Vergleich

Zum Schluss wurden die drei Varianten gegenübergestellt.

	Variante 1	Variante 2	Variante 3
	DR über Regionen	DR in Region (CH N)	DR in Region (CH N) + Backup (CH W)
Minimierung Risiken	+	-	-
Technische Umsetzbarkeit	+	-	-
"Einfache" Betreibbarkeit	+	-	-
"Einfache" Testbarkeit (DR-Test)	+	-	-
Tiefe Kosten	+	-	-
Alles in der Schweiz	+	+	+



Abbildung 11 - Vereinfachter Vergleich

### DIE WICHTIGSTEN ERKENNTNISSE

DR bzw. DR-Tests in der Public Cloud werden grundsätzlich nicht einfacher.

Azure stellt für IaaS (VMs) mit Azure Site Recovery und für die meisten PaaS Services DR-Lösungen bereit.

Die Testbarkeit (DR-Test) mit live Failover und Fall-back ist nicht bei allen Services einfach möglich. Kompromisse sind notwendig, da die Azure Services nicht beliebig anpassbar sind (kann auch positiv sein).

Es ist schwer, Informationen zu den Verfügbarkeitszonen zu bekommen.

Die Enterprise-Readiness von Azure ist noch nicht in allen Bereichen gegeben.

Es findet eine schnelle Weiterentwicklung der Services statt.

### NUTZEN

Durch die Ausarbeitung der verschiedenen Varianten konnte Versicherung B eine **fundierte Entscheidung für sie eine optimierte Lösung** treffen.