# Cloud souverän gestalten:
## Praxisleitfaden für Schweizer Unternehmen



So gewinnen Sie Kontrolle,
Sicherheit und Zukunftsfähigkeit
für Ihre Infrastruktur

Die Cloud ist fester Bestandteil moderner IT-Strategien. Gleichzeitig stehen Schweizer Unternehmen vor hohen Anforderungen an **Souveränität, Compliance, Verlässlichkeit und Betriebssicherheit,** die auf den Wunsch nach **Flexibilität, Skalierbarkeit und Innovationsfähigkeit** für ihre Infrastruktur treffen.

Dass dieses Spannungsfeld nicht nur ein „IT-Thema" ist, zeigt auch der Blick auf die staatliche Ebene: Der Bundesrat hat Ende 2025 einen Bericht zur **digitalen Souveränität** verabschiedet – als Reaktion auf die wachsende Bedeutung digitaler Ressourcen und die zunehmende Abhängigkeit von grossen Anbietern und technologisch dominierenden Nationen. Im Kern geht es dabei um **Handlungsfähigkeit:** die Fähigkeit, digitale Ressourcen aktiv zu steuern, Risiken zu erkennen und die Kontrolle über kritische Abhängigkeiten zu behalten.

Was der Bundesrat für die Schweiz insgesamt beschreibt, gilt auch für Schweizer Unternehmen: Wer seine Betriebsprozesse digital absichern und weiter skalieren will, muss seine IT so gestalten, dass **Kontrolle, Verantwortung und Sicherheit** jederzeit gewährleistet bleiben – auch dann, wenn Plattformen, Services und Teile des Betriebs ausgelagert sind.

Genau hier setzt der Begriff der **souveränen Cloud** an. Souverän meint: **bewusst entscheiden,** welche Daten und Workloads wohin gehören, und diese Entscheidung so abzusichern, dass sie im Alltag zuverlässig funktioniert.

Das umfasst im Kern drei Dinge, die in vielen Cloud-Projekten zu spät (oder zu abstrakt) betrachtet werden:

01 **Datenkontrolle:**
Welche Daten sind vorhanden, welcher Schutzbedarf gilt und wer kann wann worauf zugreifen?

02 **Betriebsfähigkeit:**
Wer ist wofür verantwortlich – fachlich, technisch und organisatorisch – und wie läuft der Betrieb im Ernstfall (Incident, Audit, Ausfall)?

03 **Abhängigkeiten & Handlungsfreiheit:**
Welche Bindungen entstehen (Provider-Services, Plattform-Lock-in, Drittsysteme) und wie bleibt ein realistisches Exit-Szenario möglich?



## Was Sie in diesem Praxisleitfaden erwartet

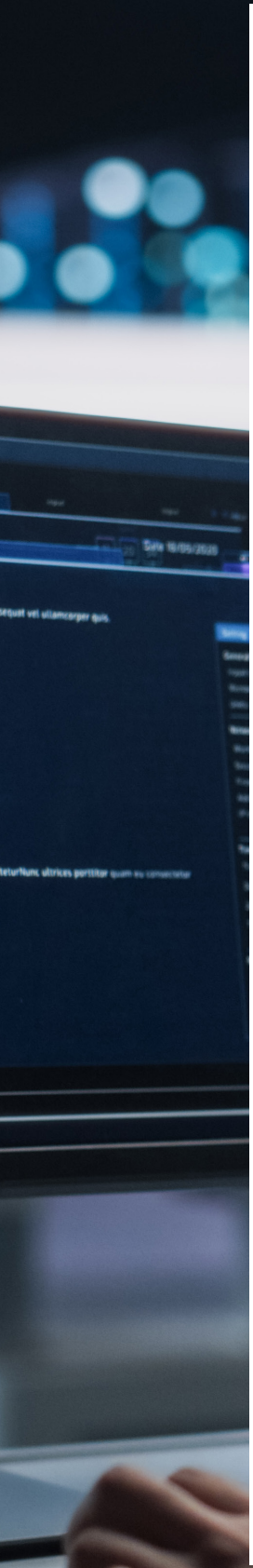
Dieser Leitfaden ist bewusst **praxisnah** aufgebaut: Er soll Ihnen Antworten auf diese wichtigsten Fragen liefern und Ihnen Orientierung geben. Sie erhalten damit einen kompakten Überblick, wie Sie eine souveräne Cloud-Strategie so aufsetzen, dass sie **skaliert** und zugleich **steuerbar** bleibt.

### WAS SIE KONKRET ERWARTET

- Einordnung der typischen Ausgangslage in Schweizer Unternehmen und Überblick über die häufigsten Herausforderungen.
- Aufdeckung typischer Denkfehler, die am Anfang plausibel wirken, später aber oft zu Mehrkosten, Sicherheitslücken oder Reibungsverlusten im Betrieb führen.
- Ableitung klarer Leitprinzipien, die souveräne Cloud-Strategien in der Praxis robust und dauerhaft steuerbar machen.
- Konkrete Leitfragen als Entscheidungshilfe, um Cloud-Vorhaben von Beginn an sauber zu strukturieren, ohne sich in Details zu verlieren.
- Ein praxiserprobtes Modell, mit dem aus Orientierung eine umsetzbare Roadmap entsteht.

Der Leitfaden ist damit eine Arbeitsgrundlage für CIOs, IT-Leitungen und Infrastrukturverantwortliche, die ihre Cloud-Umgebung bewusst gestalten wollen – als sicheres Fundament für die digitale Entwicklung ihres Unternehmens.





02

# Ausgangslage: Typische Herausforderungen in Schweizer Unternehmen

In der Praxis starten Cloud-Initiativen selten auf der „grünen Wiese". Die IT-Landschaft ist meist historisch gewachsen, die Unternehmensführung erwartet schnellere Bereitstellung und höhere Verfügbarkeit, gleichzeitig steigen Sicherheits- und Compliance-Anforderungen. In diesem Umfeld zeigen sich immer wieder ähnliche Hürden:

- **Unklarheit über Daten und Schutzbedarf**
  Viele Unternehmen haben kein vollständiges Bild darüber, **welche Daten wo liegen,** wie sie verarbeitet werden und welcher **Schutzbedarf** tatsächlich gilt. Ohne saubere Datenklassifikation werden Architektur- und Betriebsentscheidungen schnell zu Annahmen – und damit zu einem Risiko, das sich erst beim Audit oder schlimmer noch bei einem Security-Vorfall zeigt.

- **Spannungsfeld Public Cloud vs. eigenes Rechenzentrum**
  Die zentrale Frage lautet häufig nicht „Cloud oder nicht", sondern: **Welche Workloads gehören wohin – und warum?** Legacy-Systeme, Abhängigkeiten zu Applikationen, Latenzanforderungen oder sensible Daten führen dazu, dass hybride Modelle entstehen. Entscheidend ist, diese Mischung bewusst zu gestalten, statt unkontrolliert „nebenbei" entstehen zu lassen.

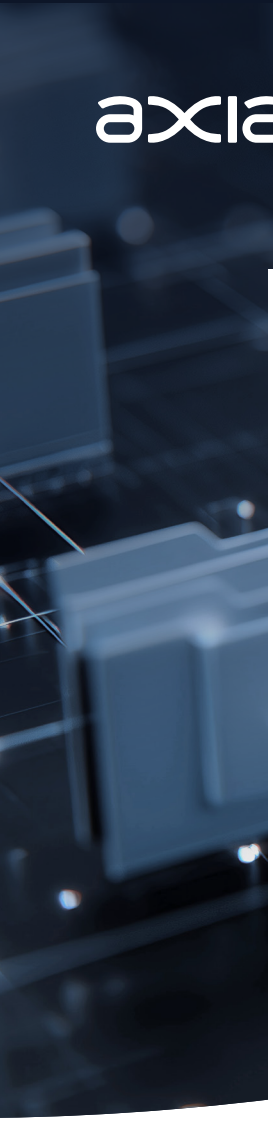
- **Regulatorische und rechtliche Anforderungen**
  In der Schweiz spielen Datenschutz, Governance sowie Branchenvorgaben eine besonders grosse Rolle. Hinzu kommen Unsicherheiten rund um internationale Rechtsräume und Zugriffsfragen. Das führt in vielen Organisationen zu einem Spagat: Man will moderne Services nutzen, muss aber **Nachvollziehbarkeit, Kontrollierbarkeit und Verantwortlichkeiten** sauber belegen können.

- **Betriebliche Komplexität**
  Hybride Umgebungen erhöhen den Koordinations- und Steuerungsaufwand deutlich: mehr Schnittstellen, mehr Beteiligte, mehr Abhängigkeiten. Ohne klare Betriebsprozesse und ein gemeinsames Verständnis von Zuständigkeiten entstehen schnell Reibungsverluste.

- **Ressourcen & Know-how**
  Interne IT-Teams stossen bei Betrieb, Governance und Weiterentwicklung zunehmend an Kapazitätsgrenzen – gerade dann, wenn parallel Modernisierung, Security-Anforderungen und Kostensteuerung bewältigt werden müssen. Häufig fehlt schlicht die Zeit, um Betriebsmodelle, Skills und Verantwortlichkeiten konsequent nachzuziehen.

Diese Ausgangslage ist der Grund, warum viele Cloud-Projekte zwar technisch starten – aber später an Erwartungen, Zuständigkeiten oder Komplexität scheitern.





03

# Typische Denkfehler – und warum sie später teuer werden

Denn oft wirken Cloud-Lösungen „einfach“: Services sind schnell gebucht, Plattformen skalieren scheinbar automatisch, und ein Teil der Verantwortung liegt ja beim Provider. Genau hier entstehen Denkfehler, die später zu Mehrkosten, Sicherheitslücken oder Betriebsproblemen führen:

» **„Der Provider macht das schon.“**
Cloud entlastet – aber sie nimmt Unternehmen nicht aus der Verantwortung. Datenschutz, Governance und viele Sicherheitsaufgaben bleiben intern oder werden geteilt. Wenn das nicht klar geregelt ist, entsteht im Alltag ein gefährliches Vakuum: Niemand fühlt sich zuständig, Aufgaben werden doppelt oder gar nicht erledigt.

» **„Cloud ist automatisch günstiger.“**
Cloud kann wirtschaftlich sein – aber nur mit sauberer Steuerung. Ohne klare Regeln für Nutzung, Skalierung, Lizenzen und Storage wächst die Umgebung schnell „organisch“ – und damit auch die Kosten. Der Effekt zeigt sich oft zeitverzögert: nicht in der Pilotphase, sondern erst nach einem Jahr Betrieb.

» **„Wir migrieren schnell – den Rest machen wir später.“**
Time-to-Cloud ist verlockend. Wenn jedoch Betriebsmodell, Sicherheitsniveau, Backup/Recovery oder IAM erst nach der Migration betrachtet werden, wird aus Tempo später teure Nacharbeit. Viele Probleme entstehen genau dann, wenn ein Setup produktiv genutzt wird – nicht beim Proof of Concept.

» **„Lift & Shift reicht.“**
Hybride Umgebungen erhöhen den Koordinations- und Steuerungsaufwand deutlich: mehr Schnittstellen, mehr Beteiligte, mehr Abhängigkeiten. Ohne klare Betriebsprozesse und ein gemeinsames Verständnis von Zuständigkeiten entstehen schnell Reibungsverluste.

» **„Wir wissen schon, welche Daten wohin dürfen.“**
In vielen Organisationen fehlt eine belastbare Datenklassifikation. Dann wird Cloud-Nutzung zur Annahme statt zur Entscheidung. Im schlimmsten Fall liegt ein Workload später „falsch“ – oder es fehlen Nachweise und Transparenz, wenn Fragen zu Zugriff, Verarbeitung oder Subunternehmern kommen.

» **„Souveränität = Datenstandort.“**
Datenlokalität ist wichtig – aber nicht allein entscheidend. Souveränität zeigt sich auch in der Governance: Wer kann zugreifen? Wie werden Änderungen kontrolliert? Wie sieht ein Exit aus? Ohne diese Fragen bleibt der vermeintlich „souveräne“ Ansatz im Alltag schwer steuerbar.

04

# Leitprinzipien einer souveränen Cloud

Souveränität entsteht also nicht durch ein einzelnes Produkt oder einen bestimmten Betriebsort. Sie entsteht durch klare Prinzipien, die Architektur, Betrieb und Governance zusammenhalten – unabhängig davon, ob Workloads in der Public Cloud, in einer Private Cloud oder in hybriden Umgebungen laufen.

Die folgenden Leitprinzipien helfen Ihnen dabei, Entscheidungen nachvollziehbar zu treffen und Ihre Cloud-Umgebung dauerhaft steuerbar zu halten.



## Datenhoheit als Ausgangspunkt

Definieren Sie früh, welche Daten Sie verarbeiten, welchen Schutzbedarf Sie haben und welche Regeln für Zugriff, Speicherung und Verarbeitung gelten.



## Klare Verantwortlichkeiten statt Grau-Zonen

Souveräne Cloud braucht eindeutige Zuständigkeiten: Wer ist wofür verantwortlich – beim Betrieb, bei Anpassungen, bei Security-Aufgaben, bei Vorfällen? Je klarer das Modell, desto stabiler wird der Betrieb im Alltag.



## Sicherheit und Compliance „by design“

Sicherheitsniveau und Compliance-Anforderungen dürfen nicht nachträglich „aufgesetzt“ werden. Logging, IAM, Verschlüsselung, Monitoring und Nachweise müssen von Beginn an Teil des Zielbilds sein.



## Betriebsfähigkeit vor Funktionsvielfalt

Eine Lösung ist nur so gut wie ihr Betrieb: Prozesse, Monitoring, Eskalation, Recovery und Dokumentation müssen realistisch umsetzbar sein – mit den vorhandenen Ressourcen und Partnern.



## Transparenz über Kosten und Nutzung

Cloud-Modelle bleiben nur dann wirtschaftlich, wenn Nutzung, Skalierung und Services aktiv gesteuert werden. Kostenkontrolle ist am Ende kein Controlling-Thema, sondern ein Betriebsprinzip.



## Interoperabilität und Exit mitdenken

Handlungsfreiheit bedeutet, Abhängigkeiten zu kennen und Alternativen zu haben. Standards, saubere Schnittstellen und ein realistisches Exit-Szenario gehören zur souveränen Planung – auch wenn ein Wechsel nicht geplant ist.

> Diese Prinzipien wirken am stärksten, wenn sie als gemeinsame Leitplanke für alle Entscheidungen verstanden werden – von der Zielarchitektur bis zum täglichen Betrieb.



05

# 12 Leitfragen für Ihre Infrastruktur-Entscheidung

Diese Prinzipien werden aber erst dann wirksam, wenn sie in konkrete Entscheidungen übersetzt werden. Die folgenden Leitfragen sollen Ihnen dabei helfen, Ihr Cloud- Vorhaben von Anfang an sauber zu strukturieren – ohne sich in Details zu verlieren.

## A) Daten & Schutzbedarf

- Welche Daten verarbeiten wir – und wie sind sie klassifiziert?
- Welche Daten/Workloads müssen aus fachlicher und regulatorischer Sicht wohin?
- Wer hat wann Zugriff – und wie wird das kontrolliert und nachgewiesen?

## B) Verantwortung & Governance

- Wer ist wofür verantwortlich (RACI) – im Normalbetrieb und im Krisenfall?
- Wie sehen Entscheidungs- und Eskalationswege aus?
- Wie wird der Service-Schnitt beschrieben – inklusive Grenzen und Abhängigkeiten?

## C) Sicherheit, Resilienz, Betrieb

- Welches Sicherheitsniveau muss mindestens gelten – und wie wird es geprüft?
- Wie sind Backup & Recovery geregelt (RPO/RTO) – und wird das getestet?
- Ist der Betrieb realistisch umsetzbar – mit den vorhandenen Ressourcen?

## D) Abhängigkeiten & Handlungsfreiheit

- Welche Abhängigkeiten entstehen durch Plattform-Services, Lizenzen und Integrationen?
- Wie sieht ein Exit-Szenario aus – technisch, organisatorisch und vertraglich?
- Wie behalten wir langfristig Kontrolle über die Kosten?

06

# Vorgehensmodell: Von der Orientierung zur umsetzbaren Roadmap

Aus diesen Leitfragen ergibt sich direkt ein Vorgehen, das in der Praxis besonders gut funktioniert: erst Klarheit schaffen, dann Entscheidungen absichern – und anschliessend Schritt für Schritt umsetzen. So entsteht eine souveräne Cloud-Strategie, die nicht nur technisch überzeugt, sondern auch im Betrieb funktioniert.

1

## Schritt 1: Ausgangslage und Schutzbedarf klären

Bevor über Zielarchitektur oder Plattformen gesprochen wird, braucht es ein belastbares Bild der Realität: Welche Systeme und Daten gibt es, welche Abhängigkeiten bestehen, welche Risiken sind sichtbar? Dazu gehört auch eine pragmatische Datenklassifikation und die Klärung, welche Workloads aus fachlicher oder regulatorischer Sicht besondere Anforderungen haben.

2

## Schritt 2: Anforderungen und Zielbild definieren

Im zweiten Schritt werden Business-Ziele, Betriebsanforderungen und Sicherheits-/Compliance-Vorgaben zusammengeführt. Daraus entsteht ein Zielbild, das beantwortet: Welche Workloads gehören wohin – und welche Prinzipien gelten dabei (z.B. Sicherheitsniveau, Verantwortlichkeiten, Resilienz)?

3

## Schritt 3: Architektur- und Betriebsmodell festlegen

Jetzt wird die entscheidende Brücke gebaut: vom Zielbild zur Realität. Welche Architektur ist passend – und vor allem: wie wird sie betrieben? Rollen (RACI), Service- Schnitt, Prozesse, Monitoring, Backup/Recovery und Eskalationen werden so beschrieben, dass sie im Alltag umsetzbar sind – auch in Co-Managed- oder Multi- Provider-Konstellationen.

4

## Schritt 4: Lösungen evaluieren und schrittweise umsetzen

Erst wenn Zielbild und Betriebsmodell klar sind, lohnt sich die konkrete Evaluation. Proof of Concepts dienen dann nicht der „Machbarkeit“, sondern dem Abgleich mit den definierten Anforderungen. Die Umsetzung erfolgt bevorzugt iterativ: priorisierte Workloads, klare Migrationswellen, sauberes Testing und dokumentierte Übergaben in den Betrieb.

5

## Schritt 5: Betrieb stabilisieren und kontinuierlich optimieren

Souveränität ist kein endgültiges Ergebnis nach Projektabschluss, sondern ein Betriebszustand. Nach dem Go-live geht es darum, Security-Niveau, Kostensteuerung und Resilienz laufend zu überprüfen – inklusive regelmässiger Recovery-Tests, Reviews der Verantwortlichkeiten sowie Optimierung von Nutzung und Architektur.

07

# Warum Axians für Sie der richtige Partner ist

Die Roadmap zeigt, **was** zu tun ist. Die entscheidende Frage in der Praxis ist jedoch, **wie** Sie diese unter realen Bedingungen umsetzen – in gewachsenen IT-Landschaften, parallel zum Tagesgeschäft, mit knappen Ressourcen und steigenden Anforderungen an Sicherheit, Compliance und Verfügbarkeit.

Genau an diesem Punkt ist die Wahl des richtigen Umsetzungspartners entscheidend. Denn eine souveräne Cloud entsteht nicht durch einzelne Massnahmen, sondern durch das Zusammenspiel aus Zielbild, Architektur, Security, Betrieb und kontinuierlicher Optimierung.

**Axians** unterstützt Schweizer Unternehmen genau hier: von der strategischen Einordnung über die Umsetzung und dank Managed Services auch bis zum verlässlichen Betrieb. Wir bringen dabei drei Ebenen zusammen, die in Cloud-Vorhaben erfahrungsgemäss den Unterschied machen:

- **End-to-End statt Stückwerk:** Strategie/Zielbild, Architektur, Migration, Security und Betrieb greifen ineinander – damit keine Lücken zwischen Konzept und Alltag entstehen.
- **Betriebsfähigkeit als Leitprinzip:** Wir denken Verantwortlichkeiten, Prozesse, Monitoring, Resilienz und kontinuierliche Optimierung von Anfang an mit – inkl. Managed Operations (Incident/Lifecycle), Backup & Recovery mit definierten RTO/RPO sowie FinOps für transparente, steuerbare Kosten.
- **Schweizer Kontext:** Persönliche und lokal verfügbare Ansprechpartner und ein klares Verständnis für Datensouveränität in der Schweiz – inkl. Betrieb in der Schweiz und Datenhaltung in Schweizer Rechenzentren sowie DSG-konforme, nachvollziehbare Security- und Governance-Strukturen.

So entsteht eine souveräne Cloud-Umgebung, die nicht nur modern ist und Ihren aktuellen Anforderungen gerecht wird, sondern die auch in Sachen Kosten, Sicherheit, Zugriffskontrolle und Weiterentwicklung dauerhaft funktionsfähig ist.





08

# Ihre nächsten Schritte mit Axians

Sie möchten herausfinden, wie Sie Ihre Infrastruktur – ob Cloud, hybrid oder on-prem – souverän aufstellen und welche nächsten Schritte für Ihre Ausgangslage jetzt wirklich sinnvoll sind?

Vereinbaren Sie ein kostenloses Erstgespräch, um Ihre Anforderungen zu klären und nächste Massnahmen zielgerichtet zu priorisieren.

## Melden Sie sich dafür einfach bei uns