Datensouveranität und Innovation dank Hybrid-Cloud-Ansatz

Ein Praxisleitfaden für Banken und Versicherungen, wie Kontrolle, Sicherheit und Flexibilität in der Cloud erfolgreich vereint werden.

Vorwort

Die Diskussion über Cloud wird noch immer häufig als reine Technologiefrage geführt. Für Banken und Versicherungen geht es jedoch um weit mehr: um Sicherheit, regulatorische Verantwortung, digitale Souveränität, Wirtschaftlichkeit und letztlich um die Fähigkeit, Innovation kontrolliert und nachhaltig voranzutreiben.

Gerade im stark regulierten Schweizer Finanzmarkt braucht es deshalb einen differenzierten Blick. Nicht jeder Workload gehört in die Public Cloud, und nicht jede bestehende Plattform muss grundlegend ersetzt werden. Entscheidend ist vielmehr, Anwendungen, Daten und Betriebsmodelle dort zu verankern, wo sie technologisch, wirtschaftlich und regulatorisch am besten aufgehoben sind. Die hybride Cloud schafft dafür einen flexiblen und zugleich kontrollierbaren Rahmen.

Damit dieser Ansatz sein Potenzial entfalten kann, müssen Architektur, Sicherheit, Compliance, Kostensteuerung und Betrieb konsequent zusammengedacht werden. Die hybride Cloud ist deshalb kein Kompromiss zwischen Innovation und Kontrolle, sondern ein strategisches Betriebsmodell, das beide Anforderungen miteinander verbindet.

Dieses Paper zeigt auf, welche Faktoren dabei berücksichtigt werden müssen, wo die grössten Hebel liegen und weshalb Cloud-Entscheidungen heute zu einer zentralen Managementaufgabe geworden sind. Ich wünsche Ihnen eine anregende Lektüre und wertvolle Impulse für Ihre eigene Cloud-Strategie.

Torsten Böttjer Senior Strategic Project Manager Technology Services, August 2026

Inhaltsverzeichnis

Hybride Cloud für Banken & Versicherer: Es geht um mehr als Technologie

Wer über IT-Outsourcing spricht, muss auch über die Cloud sprechen. Und wer Cloud sagt, meint oft die klassischen Public-Cloud-Angebote der grossen US-Anbieter. Doch in regulierten, komplexen Umfeldern, in denen hochsensible Daten im Spiel sind, ist das zu kurz gedacht. In diesem Paper zeigen wir auf, wie Banken und Versicherungen dank der hybriden Cloud höchste Sicherheitsniveaus gewährleisten, die regulatorischen Anforderungen der Schweiz einhalten sowie Skalierbarkeit und Kosteneffizienz sicherstellen.

Der Schweizer Finanzplatz steht unter doppeltem Druck: Auf der einen Seite beschleunigen FinTechs und internationale Player die Taktung der Innovation, auf der anderen Seite steigen die Anforderungen bezüglich Regulatorik, Sicherheit und Kostendisziplin. Anbieter befinden sich also in einem strategischen Spannungsfeld.

Geschwindigkeit gewinnt Marktanteile, Vertrauen hält sie

Kunden erwarten heute Services in Echtzeit, personalisierte Angebote und nahtlose Erlebnisse auf jedem Kanal, zu jedem Zeitpunkt, auf jedem Gerät. Wer mithalten will, braucht skalierbare Technologie-Plattformen, kurze Release-Zyklen und die Fähigkeit, Daten über Silos hinweg zu orchestrieren.

Gleichzeitig sind Sicherheit, Resilienz, Compliance und Revisionsfähigkeit schlicht nicht verhandelbar. Die Anforderungen der Branche sind aussergewöhnlich gross und verlangen Kontrolle, Transparenz und saubere Governance – gerade dann, wenn Workloads ausserhalb des eigenen Rechenzentrums betrieben werden. Es stellt sich die Frage: Innovation oder Compliance? Time-to-Market oder Souveränität?

Mehr als eine Infrastrukturentscheidung

Die Antwort auf dieses Dilemma ist keine reine Technologie-, sondern eine Betriebs- und Transformationsentscheidung: die hybride Cloud. Unter hybrider Cloud verstehen wir die flexible, agile Kombination von Private-/Community-Cloud-Ressourcen und Public-Cloud-Diensten. Workloads laufen dort, wo sie fachlich, regulatorisch und wirtschaftlich am besten aufgehoben sind. Sauber verbunden über standardisierte Schnittstellen, Automatisierung und einheitliche Governance. So entsteht ein Betriebsmodell, das elastische Skalierung und kontrollierte Souveränität vereint. Dieser Ansatz ist heute die Rückgrat-Architektur moderner, regulierter IT in Banken und Versicherungen.

Während die Public Cloud bei Arbeitsplatzlösungen Einzug hält, verbleiben geschäftskritische Systeme wie Kernbankenapplikationen oder E-Banking weiterhin in kontrollierten Umgebungen. Aktuell betreiben Schweizer Banken etwas weniger als die Hälfte ihrer kritischen Workloads in eigenen Rechenzentren, die andere Hälfte wurde auf Private und Community Clouds verlagert.

Zusammen, was zusammengehört – getrennt, was auseinander muss

An vielen Orten besteht heute ein heterogener Mix aus Kernbank- oder Bestandsführungssystemen, Data Warehouse und Zahlungsverkehrs-Plattformen, Fachapplikationen und neuen Analytics-/AI-Workloads. Das ist aus Sicht der Governance, Sicherheit und nicht zuletzt Kosten alles andere als ideal. Die hybride Cloud «ordnet» diese Welten:

- Kritische Kernsysteme und sensible Daten bleiben in einem hochverfügbaren, in der Schweiz betriebenen Private-/Community-Cloud-Segment – mit klaren Betriebs-, Sicherheits- und Audit-Prozessen.
- Innovationsnahe Workloads und Experimentierfelder nutzen Public-Cloud-Services für schnelle Skalierung, moderne Toolchains und globale Ökosysteme.
- Einheitliche Plattform- und Service-Governance stellt sicher, dass Deployments, Policies, Monitoring und FinOps über alle Umgebungen hinweg konsistent sind.

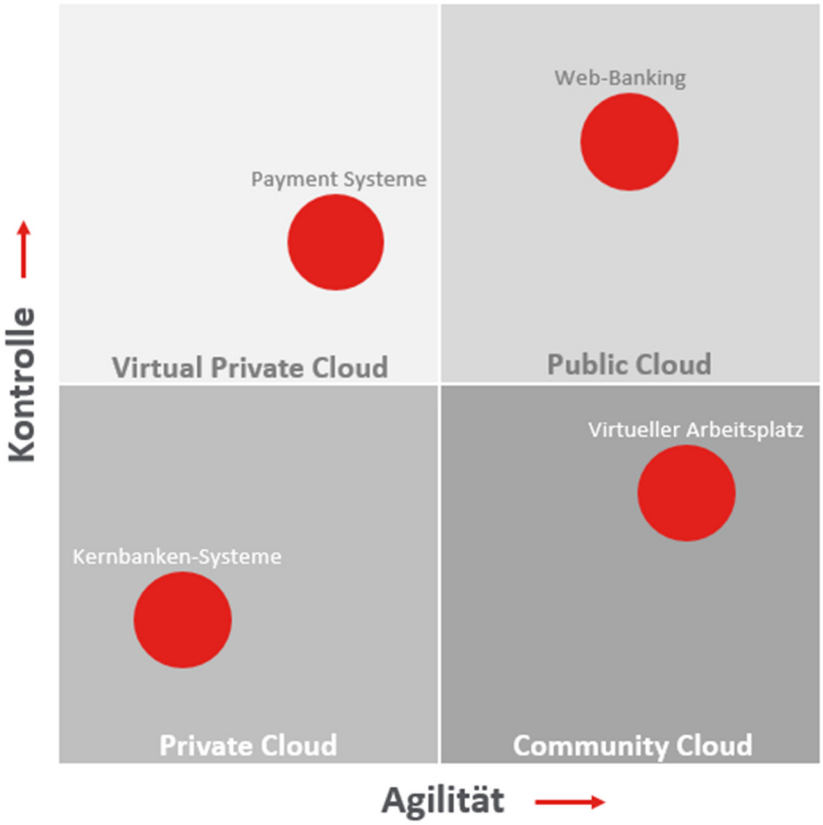

Abbildung 1: Agilität & Kontrolle im Cloud-Kontext

Für Entscheider heisst es nicht länger «Cloud – ja oder nein». Sie sind frei in der Wahl, Workloads zu verteilen. Aus dieser Perspektive ist das Thema «Cloud» eine Management-Disziplin.

Für Schweizer Banken und Versicherer ist die hybride Cloud kein Nice-to-have, sondern die strategische Schaltstelle zwischen Wachstumsambitionen und regulatorischer Sorgfalt. Sie ermöglicht

- schnelle Innovation, wo der Markt sie verlangt,
- Kontrolle und Nachweisbarkeit, wo Regulatorik und Risiko es fordern,
- und finanziell steuerbare Skalierung über Private-, Community- und Public-Clouds.

Kurz gesagt: Agilität, wo Wachstum entsteht, Souveränität, wo Regulierung verlangt ist.

Gleichzeitig Sicherheit und Flexibilität in der hybriden Cloud – geht das wirklich?

Sicherheit in der hybriden Cloud ist kein Feature oder Produkt. Sie ist ein Betriebsprinzip. In einem streng regulierten Umfeld wie dem Schweizer Finanzmarkt muss Sicherheit architektonisch verankert, operativ nachweisbar und auditfähig dokumentiert sein, immer über Private-, Community- und Public-Cloud hinweg. Genau hier spielt ein gemanagtes, regionales Hybrid-Modell seine Stärken aus.

Was «sicher» in der hybriden Cloud bedeutet

Innovationsdruck auf der einen, Regulatorik und Nachweisbarkeit auf der anderen Seite. Banken und Versicherer gewinnen dank hybrider Cloud-Strategie sowohl Agilität als auch Sicherheit, ohne Kompromisse bei regulatorischer Compliance einzugehen. Um dies zu erreichen, reicht es nicht aus, lediglich Technologien bereitzustellen. Entscheidend ist vielmehr das begleitende Management der Applikationen. Cloud-Anbieter müssen aktive Sparringpartner für ihre Kunden sein.

Die Grundprinzipien der Sicherheit in der Cloud

Die Sicherheit hybrider Cloud-Architekturen beginnt nicht mit einzelnen Technologien, sondern mit einem klaren Grundprinzip: die richtige Aufgaben- und Vertrauensverteilung zwischen privater und öffentlicher Infrastruktur. Unternehmenskritische Workloads, regulatorisch sensible Daten oder Systeme mit hohen Integritätsanforderungen benötigen eine Umgebung, deren Kontrolle vollständig beim Betreiber liegt – typischerweise ein privates Rechenzentrum oder eine isolierte Private Cloud. Gleichzeitig dienen Public Clouds als vorgelagerte Sicherheitsbarriere: Sie absorbieren DDoS-Angriffe am Edge, setzen automatisierte Threat-Detection ein, validieren Protokoll- und API-Aufrufe schon vor dem Eintritt ins private Netzwerk und entlasten damit die eigene Infrastruktur erheblich. Der Kern sicherer Hybrid-Cloud-Architekturen liegt also in einer bewussten Topologieentscheidung: Was gehört in die private Infrastruktur, wo Eigentum und Kontrolle klar geregelt sind? Und welche Teile der Applikation profitieren von der Offenheit und Skalierbarkeit der Public Cloud, ohne Sicherheits- oder Compliance-Anforderungen zu verletzen?

Eine durchdachte Segmentierung zwischen diesen Bereichen – im Netzwerk, im Identity Management, in den Datenflüssen und in den Deployment-Pipelines – schafft Klarheit, reduziert Angriffsflächen und verhindert unnötige Abhängigkeiten. So entsteht eine Architektur, in der sich Public und Private Cloud nicht gegenseitig kompromittieren, sondern ergänzen: Die Private Cloud schützt das Herzstück der Organisation, während die Public Cloud Reichweite, Agilität und Innovation ermöglicht.

Konkrete Schritte zur Verbesserung der Sicherheit

Zwei Begriffe zählen für Entscheider in diesem Kontext besonders: Datenresidenz (wo Daten physisch gespeichert werden) und Schlüsselhoheit (wer die kryptografischen Schlüssel kontrolliert). In der Praxis bedeutet das: standardmässige Verschlüsselung sowohl bei gespeicherten Daten wie auch bei der Datenübertragung («at rest» und «in transit»), klare Trennung von Domänen, regelmässige Rotation

sowie – wo sinnvoll – «Bring Your Own Key» (BYOK: Kunden liefern den Schlüssel) oder «Hold Your Own Key» (HYOK: Schlüssel verbleiben ausschliesslich unter Kunden-Kontrolle). Diese Muster müssen im Schweizer Rechtsraum umgesetzt werden, und kritische Daten müssen in Schweizer Rechenzentren bleiben, während innovationsnahe Workloads gezielt Public-Cloud-Dienste nutzen können.

Erkennen ist gut, konkrete Taten sind besser: Logs, Metriken und Traces, also die Beobachtbarkeit der Plattform, werden konsistent gesammelt und miteinander in Beziehung gebracht. Wichtig ist, dass daraus konkrete Playbooks entstehen: Wer informiert wen? Welche Systeme werden isoliert? Wie erfolgt die forensische Sicherung? Spätestens hier zahlt sich ein gemanagter Betrieb aus, bei dem nicht nur die Tools bereitgestellt, sondern der ganze Betrieb mit Security-Operations-Kompetenz für Banken und Versicherungen orchestriert wird.

Der häufig missbrauchte Begriff «Resilienz» verdient zudem ein genaueres Hinsehen. Resilienz ist mehr als «Backups haben». Es geht um unveränderbare Kopien, um getrennte Zonen, um Wiederherstellungstests, die tatsächlich geübt werden – technisch wie organisatorisch. Das setzt georedundante Schweizer Rechenzentren voraus und ein Betriebsmodell, das Wiederanlaufzeiten (RTO) und Datenverlusttoleranzen (RPO) realistisch einhält.

Schliesslich müssen wir über Governance und Nachweisbarkeit sprechen. Statt Evidenz in Excel nachzupflegen soll gelten: Richtlinien sind automatisiert prüfbar, Infrastruktur-Änderungen nachvollziehbar und Verantwortlichkeiten klar zugeordnet. Genau hier hilft ein Schweizer Community-Cloud-Modell mit Branchen-DNA: Auslagerungsvorgaben, Datenschutz und Revisionsfähigkeit werden operativ adressiert, nicht nur vertraglich. Zertifizierungen mit anerkannten Standards unterstützen Prüfbarkeit und Governance zusätzlich.

Warum ein gemanagtes, regionales Hybrid-Modell den Unterschied macht

Die Sicherheit einer hybriden Umgebung steht und fällt mit der Orchestrierung: Architektur, Betrieb, Sicherheitskontrollen, Audits und Kostensteuerung müssen aus einem Guss sein. Inventx kombiniert in der Schweiz betriebene Community-Cloud (ix.Cloud), mehrfach redundant ausgelegte Rechenzentren und die gezielte Integration von Public-Cloud-Services, inklusive neuer Bausteine wie GPU-gestützter KI-Plattformen für sensible Daten. Entscheidend: Das End-to-End-Management von Plattform, Sicherheit, Compliance und FinOps: Dies ist ein grosser Unterschied zu reinen Infrastruktur- oder Public-Cloud-Angeboten, die in den USA entwickelt wurden und auf ein anderes Regulierungsumfeld ausgerichtet sind.

Was C-Level wirklich messen sollten – ohne Zahlensalat

Wenige, aber aussagekräftige Kennzahlen sind wichtiger als viele, die schwierig zu interpretieren sind: Abdeckung der Sicherheits-Baselines in Prozent; Zeit bis Erkennung und Zeit bis Eindämmung für priorisierte Bedrohungen; Regelmässigkeit erfolgreicher Restore-Tests; und der Anteil an automatisiert

nachweisbaren Kontrollen. Wichtig ist nicht, «noch eine Kennzahl» zu finden – wichtig ist, dass die gewählten Metriken Steuerung ermöglichen und zu Verantwortlichkeiten passen.

Fazit: Sicherheit, die Innovation ermöglicht

Hybrid macht Sicherheit nicht «einfach», aber beherrschbar: mit Zero-Trust-Prinzipien, Daten- und Schlüsselhoheit im Schweizer Rechtsraum, gelebter Betriebsresilienz und evidenzgetriebener Compliance. So entsteht ein Sicherheitsniveau, das Audits besteht – und Innovation nicht bremst, sondern ermöglicht.

Kosteneffizienz beginnt vor der Migration

Cloud wird oft mit einem einfachen Versprechen verkauft: mehr Flexibilität bei tieferen Kosten. Für Banken und Versicherungen geht diese Rechnung selten so glatt auf. Der Kostendruck steigt, gleichzeitig sind viele Landschaften von Kernsystemen geprägt, die nicht für eine beliebige Verschiebung in die Public Cloud gebaut wurden. Wer Cloud nur als Zielplattform versteht, verlagert häufig Kosten, statt sie zu senken. Kosteneffizienz beginnt deshalb früher: bei einer klaren, architekturgetriebenen Entscheidung, welcher Workload wohin gehört.

Warum «Cloud First» ökonomisch zu kurz greift

In klassischen IT-Landschaften sind Kosten weitgehend planbar. Infrastruktur wird dimensioniert, beschafft, betrieben und über Jahre abgeschrieben. Das ist nicht immer effizient, aber es passt zu Systemen mit stabiler Grundlast und klaren Ressourcenprofilen. Die Public Cloud funktioniert anders. Sie ist stark, wenn Lasten schwanken, wenn Geschwindigkeit zählt oder wenn moderne Plattformdienste rasch verfügbar sein müssen. Genau dort spielt sie ihre Stärken aus. Sie wird aber teuer, wenn Workloads dauerhaft laufen, dedizierte Hardware benötigen oder lizenzseitig ungünstig abgerechnet werden. Gerade monolithische Kernbankenlösungen und transaktionsnahe Systeme können in der Public Cloud durch vCPU-Modelle, permanente Grundlast und hohe Integrationsanforderungen massiv teurer werden als erwartet. Deshalb greift klassisches FinOps oft zu spät. Es optimiert Kosten, die bereits entstanden sind. Der grössere Hebel liegt davor: im Workload Placement. Nicht jede Applikation profitiert von Elastizität. Und nicht jede stabile Plattform ist automatisch veraltet.

Workload Placement statt nachträglicher Kostenkorrektur

Kosteneffizienz entsteht, wenn Institute ihre Applikationen nicht nach Hype, sondern nach technischer und wirtschaftlicher Logik platzieren. Stateful Kernsysteme mit stabiler Auslastung gehören in eine Umgebung, die auf Verlässlichkeit, Souveränität und planbare Kosten optimiert ist. Stateless Applikationen, kundennahe Frontends oder rechenintensive Spitzenlasten passen eher in die Public Cloud, weil sie dort skalieren können, wenn es fachlich nötig ist. Diese Differenzierung ist im Schweizer Finanzmarkt zentral. Sie verhindert, dass teure Public-Cloud-Ressourcen für Workloads blockiert werden, die kaum von ihnen profitieren. Gleichzeitig verhindert sie, dass agile digitale Services im klassischen Eigenbetrieb unnötig schwerfällig und teuer werden. Die Frage lautet also nicht: Cloud oder On Premises? Sie lautet: Welche Architektur senkt die Gesamtkosten, ohne regulatorische Resilienz zu schwächen?

Klare Trennung senkt Betriebskosten

Viele Kosten entstehen, weil Betriebskonzepte vermischt werden. Wenn klassische, stateful Applikationen und moderne, verteilte Cloud Services mit denselben Prozessen, Tools und Teams betrieben werden sollen, steigt die Komplexität. Am Ende finanziert eine Plattform die Eigenheiten der anderen mit. Ein hybrides Zielbild ist wirtschaftlich dann stark, wenn es sauber trennt. Dedizierte, transaktionsnahe Workloads werden auf stabilen Plattformen betrieben. Verteilte, stateless Services laufen dort, wo Automatisierung und Skalierung am meisten bringen. Dadurch werden Verantwortlichkeiten klarer, Betriebsmuster wiederholbarer und Kosten besser steuerbar.

Das ist keine rein technische Sicht. Für Banken und Versicherer bedeutet diese Trennung weniger Reibung im Betrieb, weniger Sonderfälle und weniger Aufwand in Audits, Changes und Incidents.

Das Netzwerk wird zur Integrationsschicht

In hybriden Landschaften entscheidet nicht nur die Platzierung der Workloads über die Kosten. Entscheidend ist auch, wie die Welten verbunden werden. Zwischen Kernsystemen, digitalen Kanälen, Zahlungsverkehr und Marktadaptern entsteht eine Integrationsschicht, die früher oft über proprietäre Middleware, Gateways und klassische Appliances gelöst wurde. Das ist stabil, aber teuer und schwerfällig. Moderne, programmierbare Netzwerke verändern diese Logik. Technologien wie eBPF oder cloud-native Networking verlagern Security, Routing und Observability näher an den Datenpfad. Damit werden Schnittstellen leistungsfähiger, transparenter und einfacher zu betreiben. Gerade bei kritischen Verbindungen senkt das nicht nur Infrastrukturkosten. Es reduziert auch Aufwand in der Fehlersuche und damit die Folgekosten von Incidents.

Community Services als wirtschaftliche Antwort

Viele Schweizer Banken und Versicherungen haben ähnliche Anforderungen. Sie brauchen lokale Kontrolle, auditfähige Prozesse und hohe Sicherheit. Gleichzeitig lohnt es sich für einzelne Institute kaum, jede Plattformkomponente selbst aufzubauen und dauerhaft zu betreiben. Hier liegt der wirtschaftliche Wert von Community Services. Dedizierte, gemeinschaftlich genutzte Infrastruktur schafft Skaleneffekte, ohne die Anforderungen an Souveränität und Compliance preiszugeben. Kosten für physische Sicherheit, Plattformbetrieb und regulatorische Nachweise verteilen sich auf mehrere Schultern. Das ist oft die realistischere Alternative zum isolierten Private-Cloud-Silo im eigenen Rechenzentrum.

Run Kosten sinken durch deklarative Infrastruktur

Der langfristig grösste Kostenblock liegt nicht in der Migration, sondern im Betrieb. Manuelle Changes, Patches, Compliance-Prüfungen und Konfigurationsabweichungen binden Ressourcen und erhöhen Risiken. In regulierten Umfeldern wird jeder Fehler teuer, fachlich wie reputationsseitig. Deklarative Infrastruktur setzt hier an. Der gewünschte Zustand wird im Code beschrieben, Abweichungen werden sichtbar und können automatisiert korrigiert werden. Updates und Security-Patches lassen sich kontrolliert ausrollen und validieren. Das senkt Run-Kosten dauerhaft und reduziert menschliche Fehlkonfigurationen. Bei klassischen Systemen ist dieser Ansatz anspruchsvoller als in modernen Cloud-Umgebungen. Er braucht tiefes Systemwissen und Engineering-Fähigkeiten, die sich für einzelne Institute nicht immer wirtschaftlich aufbauen lassen. Genau deshalb wird ein gemanagtes, gemeinschaftliches Modell auch auf der Betriebsseite relevant.

Fazit: Kosteneffizienz ist Architekturarbeit

Hybride Cloud ist dann wirtschaftlich, wenn sie nicht als Kompromiss verstanden wird, sondern als bewusstes Zielbild. Der entscheidende Hebel liegt nicht im nachträglichen Sparen, sondern in der präzisen Platzierung der Workloads, in klar getrennten Betriebsmodellen und in einer Integrationsarchitektur, die nicht selbst zum Kostentreiber wird. Für Schweizer Banken und Versicherer heisst das: Effizienz und regulatorische Resilienz gehören zusammen. Wer beides erreichen will, braucht

keine pauschale Cloud-First-Strategie, sondern eine pragmatische Architektur, die stabile Kernsysteme schützt und Innovation dort beschleunigt, wo Cloud ihren wirtschaftlichen Wert wirklich ausspielt.

Compliance und Souveränität

In der Schweizer Finanz- und Versicherungsindustrie entscheidet der konkrete Einsatz der Cloud darüber, ob Innovation skalierbar wird oder in Audit-Aufwänden, Kontrollverlust-Ängsten und Abhängigkeiten stecken bleibt. Ein genauerer Blick zeigt auf, dass Compliance und Souveränität dabei nicht die Bremse sind, sondern der Mechanismus, der Public-Cloud-Innovation überhaupt erst im regulierten Umfeld nutzbar macht.

Dieses Kapitel schliesst nun den Kreis: Compliance und Souveränität sind die Klammer, die Security, Kosten, Betriebsmodell und Governance verbindlich zusammenführt und damit Cloud-Nutzung überhaupt erst «bankentauglich» macht.

Compliance in der Cloud: Was Aufsicht und Prüfungen verlangen

Viele Anforderungen klingen technisch, sind aber im Kern Governance-Fragen:

- Wer bleibt verantwortlich?
- Wer darf was prüfen?
- Wie stellen wir Kontrolle und Fortführung sicher?

Besonders zentral sind zwei Punkte, die in Cloud-Diskussionen oft unterschätzt werden:

1. Audit- und Einsichtsrechte: FINMA, Prüfgesellschaft und Institut müssen in der Lage sein, die Einhaltung aufsichtsrechtlicher Bestimmungen beim Dienstleister zu prüfen, mit jederzeitigem, ungehindertem Einsichts- und Prüfrecht.
2. Subdienstleister und geordneter Ausstieg: Cloud ist selten «ein Anbieter». Deshalb verlangt die FINMA, dass Institute frühzeitig über den Beizug oder Wechsel wesentlicher Unterakkordanten informiert werden. Und, dass sie die Möglichkeit haben, ein Outsourcing geordnet zu beenden.

Hinzu kommt: Cloud muss auch in die Resilienzlogik passen. Mit dem Rundschreiben 2023/1 zu operationellen Risiken und Resilienz betont die FINMA u. a. Themen wie kritische Prozesse, BCM und die Behandlung kritischer Daten. Und schliesslich spielt Datenschutz in der Cloud als Rechtsrahmen und als Erwartung an Transparenz eine Doppelrolle. Das totalrevidierte Datenschutzrecht ist seit 1. September 2023 in Kraft.

Souveränität: Worum es wirklich geht

«Souveränität» wird oft auf den Datenstandort Schweiz reduziert. Das ist wichtig, aber nicht ausreichend. Für Entscheider ist Souveränität am Ende die Summe aus vier Steuerungsfähigkeiten:

- Juristische Steuerbarkeit: Welche Rechtsräume können auf Daten und Prozesse wirken (Stichwort: Foreign Lawful Access, also behördliche Zugriffe aufgrund ausländischer Gesetze)? Die SBVg führt dieses Thema explizit als Schwerpunkt im aktualisierten Cloud-Leitfaden.

- Vertragliche Steuerbarkeit: Habe ich echte Audit-, Informations- und Mitwirkungsrechte – auch bei Subdienstleistern – und eine praktikable Exit-Option?
- Technische Steuerbarkeit: Wer kontrolliert Schlüssel und Identitäten? Wie wird Datenabfluss begrenzt? Wie werden Protokolle/Evidenzen erzeugt?
- Operative Steuerbarkeit: Kann der Betrieb in Störungen fortgeführt werden, inklusive Zugriff auf die notwendigen Informationen in der Schweiz? Das ist im Outsourcing-Kontext ausdrücklich adressiert.

«Hybrid» ist besonders stark

Die Hybride Cloud ist Architekturprinzip und Kontroll- und Governance-Modell in einem. Sie erlaubt, Workloads entlang von Risiko, Regulatorik und Business-Value zu platzieren und gleichzeitig Innovation über Public-Cloud-Dienste nutzbar zu machen.

Praktisch heisst das:

- Sensible, stark regulierte Workloads laufen in einer in der Schweiz betriebenen Community-/Private-Umgebung mit klaren Betriebs- und Nachweismechanismen.
- Innovations- und Skalierungsbausteine können in Public-Cloud-Services genutzt werden – aber eingebettet in ein einheitliches Governance-, Security- und Monitoring-Regime.

Also: In der Schweiz betriebene Community Cloud für Banken und Versicherungen sowie Public-Cloud-Services, die explizit auf Automatisierung, Monitoring sowie Governance- und Sicherheitsvorgaben aufsetzen. Damit ist Compliance nicht nur nachgelagert dokumentiert, sondern direkt im Betrieb erzeugt. Die Steuerung wird zur strategischen Führungsaufgabe in der hybriden, hochregulierten IT-Welt.

Die Checkliste für das Management

Der Unterschied zwischen «Cloud nutzen» und «Cloud beherrschen» liegt im Management. Public-Cloud-Hyperscaler liefern leistungsfähige Plattformen. Diese sind jedoch global gebaut, global betrieben und adressieren nicht automatisch die Schweizer Ausprägungen von Aufsicht, Audit und Datenanforderungen.

Ein Anbieter muss also Verantwortung für Betriebsfähigkeit und Nachweisbarkeit übernehmen. Wenn Sie dieses Thema in der Geschäftsleitung pragmatisch ansprechen möchten, reichen fünf Fragen als Start:

1. Können wir jederzeit Audit- und Einsichtsrechte entlang der gesamten Leistungskette (inkl. Unterakkordanten) durchsetzen?
2. Ist unser Exit realistisch geplant – technisch, organisatorisch und vertraglich – oder nur «theoretisch möglich»?
3. Wo liegen unsere kritischsten Daten und Prozesse, und passen Standort, Schlüssel-/Identity-Kontrolle und BCM dazu?
4. Haben wir einen klaren Umgang mit Foreign Lawful Access und behördlichen Verfahren, inklusive Transparenz und Zusammenarbeit mit Providern?
5. Erzeugen wir Compliance-Evidenz «by build», also laufend, oder erst kurz vor dem Audit?

Fazit: Compliance und Souveränität als Innovations-Booster

Wer Cloud im regulierten Umfeld erfolgreich nutzt, denkt Compliance und Souveränität als Designprinzip. FINMA-Outsourcing-Anforderungen, Resilienz-Erwartungen und Datenschutz setzen den Rahmen. In der Praxis besonders kritisch: Steuerung, Datenbearbeitung, Behörden/Verfahren und Audit.

Hybride Cloud ist ein besonders wirksamer Ansatz dafür: Sie verbindet Schweizer Betriebs- und Kontrolllogik mit der Innovationskraft moderner Cloud-Services. Vorausgesetzt, sie wird gemanagt, integriert und governancefähig umgesetzt.

Schlusswort

Inventx vereint regional betriebene Plattformen mit ausgewiesener Finanz- und Versicherungskompetenz. Das Unternehmen agiert dabei nicht als Infrastruktur-Provider, sondern als Managed-Hybrid-Cloud-Partner, gezielt ausgerichtet auf die spezifischen Anforderungen von Banken und Versicherungen. Dazu gehören:

- Eine Community-Cloud in der Schweiz (ix.Cloud): für Banken und Versicherungen, mit umfassendem Service-Katalog und höchsten Anforderungen an Verfügbarkeit, Sicherheit, Performance und Resilienz.
- Der eigenständige Betrieb in vier hochverfügbaren Rechenzentren: für Souveränität, kurze Wege und Redundanz.
- Hybrid by Design: Public-Cloud-Dienste werden dort integriert, wo es geschäftlich Sinn macht. Multi-hybride Strategien inklusive sauberer Daten- und Netzwerk-Anbindung.

Wesentlich für Entscheider: Inventx managt die Lösungen vom Plattformbetrieb über Integration, Automatisierung, Security & Compliance bis zu FinOps und Service-Management. Das entlastet die Organisation, reduziert Komplexität und beschleunigt die Umsetzung geschäftlicher Prioritäten.

Wir freuen uns auf den persönlichen Dialog – ganz getreu unserer Werte Innovation, Interaktion und Swissness!

Torsten Böttjer
torsten.boettjer@inventx.ch
T +41 81 287 16 01