



White Paper

Cloud Strategie

Inhaltsverzeichnis

Executive Summary.....	4
Ausgangslage & Herausforderungen im Mittelstand.....	4
Warum Cloud? Nutzen, Grenzen & Realitätscheck.....	6
Der Entscheidungsrahmen: Das 7-Dimensionen-Modell.....	7
Recht & Sicherheit: Der unverzichtbare Compliance-Block.....	9
Rechtliche Anforderungen: Klarer, als viele denken.....	10
Sicherheit: Der kritische Erfolgsfaktor.....	10
Die fünf unverhandelbaren Security-Maßnahmen.....	11
Handlungsempfehlungen.....	11
Warum ein strategischer Partner entscheidend ist.....	12
Kosten & TCO: Wirtschaftlichkeit realistisch bewerten.....	12
Warum Cloud-Kosten so schwer zu beurteilen sind.....	13
Die wichtigsten Kostentreiber.....	13
TCO-Bewertung über 3–5 Jahre.....	14
Typische Kostenfallen im Mittelstand.....	14
Handlungsempfehlungen.....	14
Warum Sie TCO nicht allein bewerten sollten.....	15
Cloud-Betriebsmodelle: Wann Public, Hybrid oder Private sinnvoll ist.....	15
Public Cloud: maximale Flexibilität & Geschwindigkeit.....	15
Hybrid Cloud: realistische Mitte für den Mittelstand.....	16
Modernes Private Cloud / On-Prem: die unterschätzte Option.....	16
Wie Unternehmen das richtige Modell auswählen.....	17
Beratungs-Mehrwert: Warum Sie dieses Modell nicht allein aufsetzen sollten.....	17
Organisation, Rollen & Governance: Warum Strukturen wichtiger sind als Technik.....	18
Warum Organisation & Governance im Mittelstand oft fehlen.....	19
Vier unverzichtbare Rollen einer Cloud-Organisation.....	19
Governance: Der Ordnungsrahmen.....	20
Handlungsempfehlungen für den Aufbau einer Cloud-Organisation.....	21
Warum Sie Organisation & Governance nicht allein aufbauen sollten.....	21
Vorgehensmodell: Die 4 Stufen zur Cloud-Strategie.....	22
Case Studies: Drei typische Cloud-Ausgangslagen im Mittelstand.....	25
Die größten Stolperfallen (und wie man sie vermeidet).....	28

Handlungsempfehlungen in drei Transformationsphasen.....	30
Warum Sie diese Reise nicht allein machen sollten.....	32
Cloud ist ein Erfahrungsprojekt, kein Lernprojekt	33
Die größten Risiken bei Alleingang	33
Was ein strategischer Partner wirklich leistet	34
Warum frühe Einbindung entscheidend ist.....	34
Kontrolle behalten, ohne Abhängigkeit.....	35
Die Kernbotschaft	35
Unser Beratungsansatz & der Mehrwert für Ihr Unternehmen	35
Unser Grundprinzip: Strategie vor Migration.....	36
Unser Vorgehen: Struktur statt Bauchgefühl	36
Was uns von klassischen Dienstleistern unterscheidet	37
Der konkrete Mehrwert für Ihr Unternehmen.....	37
Unser Leistungsversprechen.....	38
Unser abschließendes Commitment	38

Executive Summary

Der deutsche Mittelstand steht an einem Wendepunkt.

Digitalisierung ist nicht mehr optional, sondern Grundlage für Wettbewerbsfähigkeit, Kosteneffizienz, Sicherheit und Resilienz. Gleichzeitig werden Geschäftsmodelle volatiler, Sicherheitsanforderungen steigen und Innovationszyklen werden kürzer. In dieser Situation wird die Cloud häufig als Heilsbringer vermarktet, aber die Realität ist differenzierter.

Cloud kann enorme Vorteile bieten:

- flexible Skalierung,
- bessere Sicherheitsmechanismen,
- weniger Betriebsaufwand,
- und schnellere Digitalisierung.

Doch ohne klare Ziele, ohne Governance und ohne strukturierten Ansatz führt Cloud-Einführung zu Kostenexplosion, Sicherheitsrisiken und operativem Chaos. Besonders kleine und mittlere Unternehmen haben begrenzte Ressourcen, und genau deshalb ist ein strukturierter Prozess entscheidend.

Dieses Whitepaper liefert dafür einen praxisbewährten Rahmen:

- Ein objektives Bewertungsmodell mit 7 Dimensionen, das Entscheidungssicherheit schafft.
- Konkrete Handlungsempfehlungen, wie man Sicherheit, Kosten, Compliance und Innovation in Einklang bringt.
- Ein 3-Phasen-Plan, der den Einstieg realistisch, risikoarm und kontrolliert ermöglicht.
- Fallbeispiele, die typische Szenarien im Mittelstand abbilden.
- Eine klare Empfehlung, warum externe Expertise den Unterschied zwischen Erfolg und Scheitern macht.

Denn Cloud-Transformation ist kein Infrastrukturprojekt, sie ist eine Organisationsentwicklung, die Strategie, Prozesse, Rollen, Menschen und Technologie umfasst. Und genau das ist im Mittelstand selten vollständig vorhanden.

Der entscheidende Satz lautet daher:

Unternehmen können die Cloud technisch allein einführen, aber sie erreichen die gewünschten Ergebnisse nur mit einem erfahrenen Partner, der Governance, Sicherheit, Architektur und Betrieb professionell orchestriert.

Dieses Whitepaper zeigt den Weg dorthin.

Ausgangslage & Herausforderungen im Mittelstand

Die Realität im Mittelstand ist geprägt von drei strukturellen Hemmnissen:

1. Historisch gewachsene IT-Systeme

Viele Unternehmen betreiben noch Systeme, die nie für Cloud- oder Integrationsfähigkeit gebaut wurden. Das führt zu:

- langen Migrationsprojekten,
- manuellen Prozessen,
- und fehlender Skalierbarkeit.

2. Operative Überlastung der IT

Die IT arbeitet permanent „am Limit“. Dadurch fehlt Zeit für:

- Modernisierung,
- Automation,
- Security-Härtung,
- Prozessoptimierung.

Digitalisierungsvorhaben werden dadurch nicht nur verzögert, sie scheitern oft still.

3. Wachsende Sicherheits- und Compliance-Anforderungen

Cloud reduziert viele Risiken, aber nur bei richtiger Konfiguration.

KMUs kämpfen vor allem mit:

- Identitätsrisiken,
- mangelndem Logging,
- ungetesteten Backups,
- unklaren Verantwortlichkeiten.

Warum kann der Mittelstand die Cloud nicht einfach „nebenbei“ einführen?

Weil Cloud keine Technologieeinführung ist, sondern eine Transformation.

- Rollen müssen sich verändern.
- Verantwortlichkeiten müssen neu verteilt werden.
- Kostenmodelle funktionieren anders.
- Sicherheit wird identitätszentriert.
- Governance wird zentral.
- Prozesse müssen automatisiert werden.
- Fachbereiche müssen eingebunden werden.

Diese Veränderungen sind in KMUs nicht einfach voraussetzbar. Sie müssen bewusst aufgebaut werden.

Beratungs-Mehrwert an dieser Stelle:

Ein erfahrener Partner verkürzt diesen Weg von „mehreren Jahren“ auf „wenige Monate“ und vermeidet typische kostspielige Fehler, die intern oft unentdeckt bleiben.

Warum Cloud? Nutzen, Grenzen & Realitätscheck

Die Cloud ist kein Trend und kein Marketingbegriff. Sie ist ein tiefgreifender struktureller Wandel in der Art, wie Unternehmen IT nutzen, betreiben und für Innovation einsetzen. Für viele mittelständische Unternehmen in Deutschland ist Cloud jedoch zugleich Chance und Unsicherheitsfaktor: Die Vorteile sind klar, aber der Weg dorthin ist komplexer als erwartet.

Die drei zentralen Nutzenversprechen der Cloud:

1. Flexibilität & Skalierung

Cloud-Ressourcen wachsen oder schrumpfen bedarfsgerecht und nahezu in Echtzeit.

Für Unternehmen mit saisonalen Peaks oder schwankender Auslastung ist das ein erheblicher wirtschaftlicher Vorteil.

Beispiel:

Ein E-Commerce-Unternehmen kann zur Hochsaison tausende Anfragen gleichzeitig verarbeiten, ohne zusätzliche Hardware bereithalten zu müssen.

2. Schnelleres Arbeiten & Innovation

Cloud erlaubt kurze Bereitstellungszeiten, automatisierte Deployments, standardisierte Prozesse und schnellere Updates.

Dadurch verkürzen sich Innovationszyklen deutlich.

3. Sicherheit & Resilienz

Moderne Sicherheitsmechanismen, Zero Trust und integrierte Überwachung bieten ein Sicherheitsniveau, das On-Premise für KMUs schwer erreichbar ist.

Rechenzentren sind redundant, ausfallsicher und weltweit vernetzt.

Die Grenzen der Cloud — das sagt Ihnen kaum jemand

1. Cloud ist nicht automatisch günstiger

Ohne Governance sogar schnell *deutlich teurer* als On-Prem.

Grund: Pay-as-you-go, Overprovisioning, fehlende Tagging-Standards.

2. Nicht jede Anwendung ist Cloud-ready

Alte Systeme, Maschinenanbindungen oder selbstentwickelte Anwendungen sind oft nicht migrierbar.

3. Organisation & Skills sind entscheidend

Cloud scheitert selten an Technik, sondern fast immer an Strukturen.

Identity, Prozesse, Governance und Kostenmanagement müssen reifer werden.

Realitätscheck: Warum Cloud im Mittelstand oft scheitert

- Fehlende Ziele („Wir wollen einfach moderner werden.“)
- Übersprungene Governance („Wir starten erst mal...“)
- Keine Verantwortlichkeiten
- Überlastete IT
- Mangelnde Security-Baseline
- Unklare Kostenplanung
- Zu viel „Lift & Shift“
- Fehlendes Change Management

Beratungs-Mehrwert

Unternehmen scheitern selten an Azure, AWS oder der Technik.

Sie scheitern daran, dass niemand das Projekt ganzheitlich führt, weder fachlich noch organisatorisch.

Ein erfahrener Partner...

- definiert Ziele und Rahmenbedingungen
- baut Governance und Sicherheit von Anfang an ein
- sorgt dafür, dass typische Fehler gar nicht erst passieren
- beschleunigt die Umsetzung um Monate
- reduziert Kosten, Risiken und technische Schulden
- entlastet die interne IT erheblich

Die Cloud können Sie technisch allein einführen. Eine erfolgreiche Cloud-Strategie erreichen Sie nur mit einem professionellen Partner.

Der Entscheidungsrahmen: Das 7-Dimensionen-Modell

Eine erfolgreiche Cloud-Strategie entsteht nicht durch Technologieauswahl, sondern durch eine systematische, nachvollziehbare Bewertung aller wesentlichen Einflussfaktoren. Genau dafür wurde das 7-Dimensionen-Modell entwickelt. Es dient als objektive Entscheidungsgrundlage, mit der Chancen, Risiken und Kosten transparent gegeneinander abgewogen werden können, unabhängig von Anbietern oder Architekturvarianten.

Warum ein strukturiertes Bewertungsmodell zwingend notwendig ist

Viele Unternehmen starten Cloud-Projekte aus einem diffusen Modernisierungsdruck heraus: „Wir müssen moderner werden“, „Wir wollen weg von Hardware“, „Der Anbieter empfiehlt es“. Diese Aussagen sind verständlich, aber sie ersetzen keine solide Entscheidungsgrundlage.

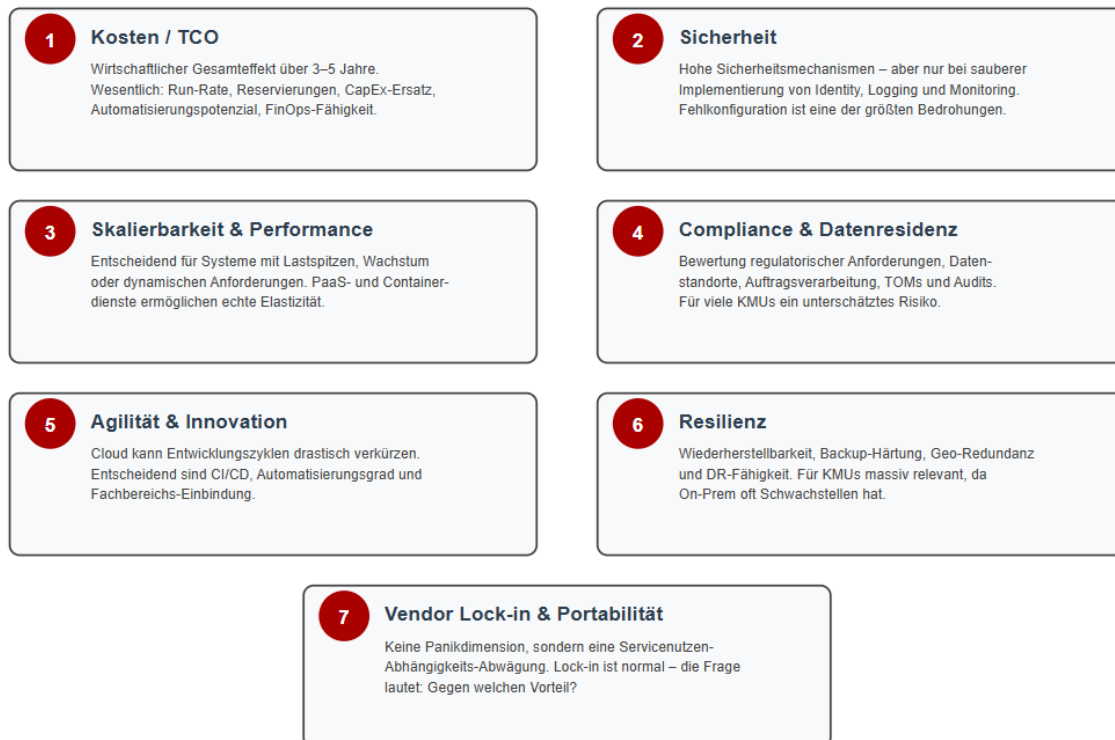
Fehlt die Struktur, entstehen typische Fehlentscheidungen:

- Workloads werden migriert, die On-Prem effizienter wären
- Kosten explodieren durch falsche Architekturwahl
- Sicherheitsrisiken entstehen durch ungeeignete Identitätsmodelle
- Governance wird zu spät aufgebaut

- Teams werden überfordert oder falsch aufgestellt
- Entscheidungen wirken inkonsistent oder politisch statt objektiv

Ein Bewertungsmodell verhindert genau das.

Die sieben Dimensionen im Überblick



Wie entsteht aus den 7 Dimensionen eine Entscheidungsgrundlage?

Jede Dimension wird auf einer Skala von 1–5 bewertet.

Daraus ergibt sich ein Profil, das:

- Public, Hybrid und Private objektiv vergleichbar macht
- interne Diskussionen versachlicht
- Investitionsentscheidungen nachvollziehbar macht
- Risiken sichtbar macht, die sonst verborgen bleiben
- die Erwartungshaltung im Management realistisch ausrichtet

Ein strukturierter Entscheidungsprozess spart Monate und hohe Kosten, weil er Fehlwege früh eliminiert.

Beratungs-Mehrwert

Ein Bewertungsmodell funktioniert nur, wenn:

- Annahmen realistisch sind
- technische und organisatorische Auswirkungen verstanden werden

- Compliance-Fragen korrekt eingeordnet werden
- Risiken vollständig identifiziert werden
- Kosten und Architektur fachlich valide bewertet werden
- Entscheidungsträger die Ergebnisse akzeptieren

Das verlangt Erfahrung, die intern oft nicht vorhanden ist.

Ein erfahrener strategischer Partner reduziert Risiko, Aufwand und Unsicherheit erheblich.

Er bringt Best Practices ein, stellt die richtigen Fragen und erkennt Fallstricke, bevor sie teuer werden.

„Wir unterstützen Sie genau in diesem Punkt: Wir moderieren, analysieren, bewerten und leiten belastbare Entscheidungen her. Ob und wie Sie danach umsetzen, liegt vollständig bei Ihnen.“

Recht & Sicherheit: Der unverzichtbare Compliance-Block

Rechtliche Anforderungen und Informationssicherheit gehören zu den meistunterschätzten Aspekten einer Cloud-Strategie. Viele Unternehmen fokussieren sich zu Beginn auf Technik, Kosten oder Geschwindigkeit, doch die eigentliche Grundlage für jede Cloud-Entscheidung ist die Fähigkeit, gesetzliche Anforderungen einzuhalten und Sicherheitsrisiken beherrschbar zu machen. Gerade im deutschen Mittelstand, in dem Vertrauen, Verfügbarkeit und Revisionssicherheit zentrale Werte sind, ist dieser Bereich erfolgskritisch.

Rechtliche Anforderungen: Klarer, als viele denken

Für den Großteil der mittelständischen Unternehmen ist Cloud im Rahmen der DSGVO problemlos möglich, sofern die Anforderungen korrekt adressiert werden.

Wesentliche rechtliche Bausteine sind:

1

Rollenverständnis (DSGVO: Verantwortlicher ↔ Auftragsverarbeiter)

Das Unternehmen bleibt Verantwortlicher.
Der Cloud-Anbieter ist Auftragsverarbeiter.
Das bedeutet: Verantwortung kann nicht delegiert werden.

2

Datenstandort und Datenresidenz

Für 95 % der Anwendungsfälle sind EU-Regionen völlig ausreichend. Wichtig ist:

- Klare Festlegung der Region (z. B. Germany West Central)
- Dokumentation der Datenflüsse
- Prüfung, ob Sonderfälle wie Gesundheitswesen, NIS2 oder KRITIS greifen

3

Auftragsverarbeitung (AVV) & TOMs

AV-Verträge müssen vollständig dokumentiert sein, inklusive:

- technischen und organisatorischen Maßnahmen (TOMs)
- Unterauftragsverhältnissen
- Löschkonzepten und Verschlüsselungsverfahren

4

Transparente Revisionsfähigkeit

Cloud macht Audits einfacher – wenn man Logging & Monitoring aktiviert.
Wenn nicht: deutlich schwieriger.

Für Entscheider wichtig:

*Rechtlich scheitert Cloud nicht – sie scheitert an fehlender Dokumentation
und fehlender Klarheit.*

Sicherheit: Der kritische Erfolgsfaktor

Cloud-Plattformen sind sicher. Unsichere Cloud-Umgebungen entstehen nicht durch Microsoft, AWS oder Google, sondern durch Kundenkonfiguration.

Die häufigsten Schwachstellen im Mittelstand sind:

- fehlende MFA-Absicherung
- unzureichende Identity Governance
- ungenutztes Zero Trust
- deaktiviertes oder unzureichendes Logging
- Backups, die zwar existieren, aber nicht wiederherstellbar sind
- kein zentrales Berechtigungsmodell
- unklare Rollen

Das größte Risiko in der Cloud ist nicht der Hacker, es ist eine Fehlkonfiguration.

Die fünf unverhandelbaren Security-Maßnahmen

1 Multi-Faktor-Authentifizierung (MFA) für alle Benutzer

Ohne MFA ist jede Cloud-Umgebung verwundbar.

MFA reduziert >99 % erfolgreicher Angriffe.

2 Conditional Access – Steuerung der Zugriffskontexte

„Wer darf wann und wie worauf zugreifen?“

Das ist die neue Perimetergrenze.

3 Privileged Identity Management (PIM)

Administrative Rechte nur „Just-in-Time“, nie dauerhaft.

4 Logging und Monitoring

Ohne Logs gibt es weder Nachweisbarkeit noch Früherkennung. Einfacher Grundsatz:

„Was Sie nicht sehen, können Sie auch nicht schützen.“

5 Gehärtete Backups und Disaster Recovery

Ransomware greift Backups zuerst an.

Unveränderliche (immutable) Backups sind Pflicht.

Handlungsempfehlungen

- Führen Sie eine Data Classification Policy ein.
- Aktivieren Sie MFA und Conditional Access unternehmensweit.
- Stellen Sie sicher, dass Administrative Konten nie dauerhaft zugewiesen sind.
- Aktivieren Sie alle relevanten Logs und halten Sie sie mindestens 90 Tage vor.
- Dokumentieren Sie AVV, TOMs und Datenflüsse.
- Definieren Sie Sicherheitsrollen und deren Verantwortlichkeiten.
- Führen Sie einen jährlichen Security- und DR-Test durch.

Warum ein strategischer Partner entscheidend ist



Recht & Sicherheit sind die Bereiche, in denen die meisten Cloud-Projekte scheitern oder verzögert werden.

Nicht wegen der Technik – sondern wegen:

- Interpretationsfehlern in der DSGVO
- fehlenden Dokumenten
- Lücken in der Identity-Architektur
- unklaren Verantwortlichkeiten
- schlecht konfigurierten Policies
- mangelnder Erfahrung im Umgang mit Compliance-Anforderungen



Ein strategischer Partner bringt:

- Struktur
- bewährte Dokumentvorlagen
- jahrelange Erfahrung aus anderen Projekten
- Wissen, welche Maßnahmen für Sie wirklich relevant sind
- und vor allem: die Fähigkeit, Risiken vorher zu erkennen

„Recht & Sicherheit sind kein Ort für Experimente.“

Wer hier Fehler macht, merkt es oft erst, wenn es zu spät ist.“

Kosten & TCO: Wirtschaftlichkeit realistisch bewerten

Kaum ein Bereich der Cloud führt zu so vielen falschen Erwartungen wie Kosten. Viele Unternehmen beginnen die Cloud-Reise mit der Annahme, die Cloud sei günstiger als On-Premises. Die Realität ist differenzierter: Cloud *kann* günstiger sein, aber nur, wenn Architektur, Governance und Betriebsmodell korrekt aufeinander abgestimmt sind. Ohne diese Grundlagen steigen Kosten nicht selten *massiv* an.

Für eine realistische Bewertung braucht es eine Total Cost of Ownership (TCO)-Perspektive, die über mehrere Jahre reicht und sowohl CapEx (Investitionen) als auch OpEx (laufende Kosten) berücksichtigt.

Warum Cloud-Kosten so schwer zu beurteilen sind

Die Komplexität entsteht durch drei strukturelle Unterschiede:

1 Kosten verschieben sich von CapEx zu OpEx

On-Prem zahlen Sie für Hardware „im Voraus“.
In der Cloud zahlen Sie für tatsächliche Nutzung – per Minute oder Sekunde.

Das sorgt für Flexibilität, aber auch für:

- schwer einschätzbare Spitzen
- unvorhersehbare Kosten
- intransparente Budgets, wenn Governance fehlt

2 Die Architektur beeinflusst die Wirtschaftlichkeit

Ein einfaches Beispiel:

Eine dauerhaft laufende VM in der Cloud kostet ungleich mehr als dasselbe System auf einem vorhandenen Server.

Wird sie hingegen nur 4 Stunden am Tag benötigt, spart sie erheblich.

3 Fehlende FinOps-Prozesse lassen Kosten entgleiten

Viele KMUs haben keinen etablierten Prozess für:

- Tagging
- Kostenstellenzuordnung
- Reserved Instances (RI)
- Optimierung von Laufzeiten
- Right-Sizing
- Abschalten ungenutzter Ressourcen

Ohne FinOps gilt:
Cloud ist immer teurer.

Die wichtigsten Kostentreiber

Folgende Faktoren beeinflussen Cloud-Kosten am stärksten:

1. Compute (VMs, Skalierung, CPU/Memory-Größen)
Größter Block, besonders bei Lift & Shift.
2. Storage (Datenbanken, Files, Backups)
Datenwachstum frisst Budget, wenn nicht überwacht.
3. Netzwerkverkehr
Besonders problematisch bei hybriden Szenarien ohne Planung.
4. Lizenzmodelle
SQL, Windows und Drittanbieter-Lizenzen wirken oft überraschend teuer.
5. Security, Logging und Monitoring
Unverzichtbar, aber oft nicht kalkuliert.

TCO-Bewertung über 3–5 Jahre

Eine seriöse Wirtschaftlichkeitsbewertung berücksichtigt:

- Investitionseinsparungen
(Server, Storage, Netzwerk, Ersatzinvestitionen)
- Betriebseinsparungen
(Patching, Monitoring, Hardwarepflege)
- Projektkosten
(Migration, Modernisierung, Workshops, Schulungen)
- Laufende Kosten
(VMs, PaaS, Netz, Datenbanken)
- Kostenoptimierungspotenzial
(Automation, PaaS, Serverless, RI/Savings Plans)
- Opportunitätskosten
(Innovation, Time-to-Market, Security, Fachkräftemangel)

Cloud rechnet sich oft nicht über reine Infrastruktur, sondern über Agilität, Geschwindigkeit und Risikoreduktion.

Typische Kostenfallen im Mittelstand

1. „Lift & Shift“ ohne Modernisierung
→ führt fast immer zu unnötig hohen Kosten.
2. Fehlendes oder falsches Tagging
→ Kosten sind nicht zuordenbar → keine Steuerung.
3. Keine Abschaltprozesse
→ Dev/QA-Umgebungen laufen nachts und am Wochenende weiter.
4. Dauerhafte öffentliche IPs und ungeplante Netzwerkgebühren
→ besonders kritisch bei Hybrid-Szenarien.
5. Keine Reservierungen
→ On-demand ist fast immer die teuerste Variante.

Handlungsempfehlungen

- Erstellen Sie eine 3–5-Jahres-TCO-Planung.
- Nutzen Sie Right-Sizing und Auto-Shutdown für nicht-produktive Workloads.
- Planen Sie Reservierungen/Savings Plans ab einer Last > 3 Monate.
- Ermitteln Sie vorab eine Baseline für Netzwerkverkehr.
- Nutzen Sie Managed/PaaS statt VMs, wo möglich.

- Führen Sie ein FinOps-Modell ein (Kostenstellen, Budgets, Alerts).

Warum Sie TCO nicht allein bewerten sollten

TCO-Bewertungen scheitern intern häufig an:

- falschen Annahmen
- fehlenden Erfahrungswerten
- unzureichender Transparenz über Kostenmodelle
- fehlendem Verständnis für Cloud-Abrechnungslogiken
- überoptimistischen Einsparungsannahmen der Anbieter
- blinden Flecken bei Netzwerk-, Backup- oder Lizenzkosten

Ein strategischer Partner bringt:

- realistische Benchmarks
- Erfahrungswerte aus vielen Projekten
- Wissen über Architektur- und Lizenzoptionen
- Validierung von Kostenmodellen
- Optimierungsansätze, die Budget schonen
- klare Handlungsempfehlungen, bevor Fehlkosten entstehen

„Eine falsche Architekturentscheidung kann Cloud-Kosten über Jahre um 40–70 % erhöhen. Eine fundierte TCO-Bewertung verhindert das, und spart ein Vielfaches der Beratungskosten.“

Cloud-Betriebsmodelle: Wann Public, Hybrid oder Private sinnvoll ist

Cloud-Entscheidungen scheitern häufig nicht an der Technik, sondern an einer falschen Grundannahme: Dass es *ein* richtiges Betriebsmodell gebe. In der Praxis existiert dieses Ideal nicht. Unternehmen entscheiden sich nicht zwischen Public *oder* On-Premises, sondern für eine Mischung aus Betriebsmodellen, die zum Geschäftsmodell, zu Compliance-Anforderungen und zum Reifegrad der Organisation passt.

Deshalb ist die Frage nicht „Welche Cloud ist die beste?“, sondern „Welches Betriebsmodell erzeugt für Ihre konkreten Workloads den größten Nutzen, und die geringsten Risiken?“

Public Cloud: maximale Flexibilität & Geschwindigkeit

Die Public Cloud ist das leistungsfähigste und innovativste Modell, insbesondere für kleine und mittelständische Unternehmen, die:

- skalierende Workloads betreiben
- Proof-of-Concepts oder neue Produkte schneller bereitstellen wollen
- geringe interne Betriebsressourcen haben
- Wert auf moderne Security-Mechanismen legen
- mobil oder verteilt arbeiten

✓ Vorteile • Hohe Agilität: Ressourcen in Minuten statt Wochen • Starke Security: Identity-first, Zero Trust, DDoS-Schutz nativ integriert • Geringer Betriebsaufwand: kein Patchen, kein Hardware-EOL • Innovationsgeschwindigkeit: Zugriff auf KI, Automatisierung, Datenservices • Pay-as-you-go: Nutzung statt Bereitstellung	⚠ Risiken/Limitierungen • Kosten steigen ohne Governance schnell an • Latenz sensibler Produktionssysteme kann zu hoch sein • Abhängigkeit von Dienstleister-Know-how • Lock-in bei proprietären Diensten (bewusst eingehen, nicht vermeiden)
→ Geeignet für: Dienstleister, Handel/E-Commerce, Webanwendungen, SaaS-first-Strategien, moderne Entwicklungs-Teams.	

Hybrid Cloud: realistische Mitte für den Mittelstand

Hybrid Cloud ist nicht Rückschritt, sondern Pragmatismus.

Sie verbindet Cloud-Flexibilität mit der Stabilität lokaler Systeme.

Dieses Modell ist ideal, wenn:

- Maschinen, Sensoren oder Produktionssysteme angebunden sind
- bestimmte Anwendungen aus Compliance- oder Lizenzgründen lokal bleiben müssen
- Historien- oder Legacy-Systeme nicht Cloud-ready sind
- Bandbreite oder Latenz limitierend wirken
- Migration schrittweise erfolgen soll

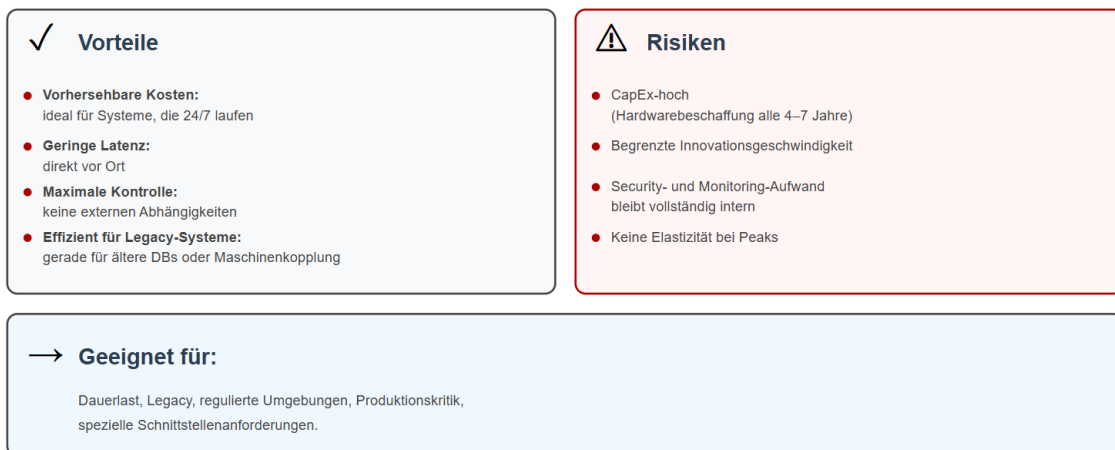
✓ Vorteile • Schrittweise Transformation: kein Big Bang, geringere Risiken • Sichere Produktionsnähe: geringe Latenz, lokale Kontrolle • Schneller Nutzen: Teile wandern in die Cloud, andere bleiben stabil • Solide TCO: Vermeidung unnötiger Neubau-Kosten	⚠ Risiken • Netzwerkkosten und Komplexität wachsen • Zwei Betriebsmodelle müssen gleichzeitig gemanagt werden • Klare Verantwortlichkeiten notwendig („Wer betreut was?“) • Security muss hybrid gedacht werden (Cloud ↔ On-Prem)
→ Geeignet für: Produktion, Fertigung, Unternehmen mit größeren On-Prem-Investitionen, alle Firmen mit Legacy-Anwendungen.	

Moderne Private Cloud / On-Prem: die unterschätzte Option

Private Cloud ist keine „alte IT“. Sie ist eine bewusste Entscheidung für:

- stabile Dauerlasten
- geringe Skalierungsanforderungen
- definierte Kosten über Jahre
- hohen Kontrollbedarf
- sensible Daten, die im Haus bleiben sollen

Moderne On-Prem-Infrastrukturen verwenden heute dieselben APIs, Tools und Automatisierungsmechanismen wie Cloud (z. B. Kubernetes, IaC).



Wie Unternehmen das richtige Modell auswählen

Die Wahl des Betriebsmodells sollte niemals von Technologie getrieben werden, sondern von:

- Geschäftsprozessen
- Workload-Kritikalität
- Compliance-Anforderungen
- Kostenstruktur (TCO-5-Jahresblick)
- Reife der Organisation
- benötigter Innovationsgeschwindigkeit
- Zukunftsfähigkeit der Architektur

Das 7-Dimensionen-Modell bildet genau diese Parameter ab und macht hybride Entscheidungen objektiv.

Beratungs-Mehrwert: Warum Sie dieses Modell nicht allein aufsetzen sollten

Der größte Fehler ist, eine Cloud-Entscheidung ausschließlich aus einer technischen Perspektive zu betrachten.

Doch Betriebsmodelle beeinflussen:

- IT-Organisation
- Kosten über Jahre
- Verantwortlichkeiten

- Security- und Compliance-Struktur
- Zukunftsfähigkeit der Architektur

Unternehmen treffen hier oft Fehlentscheidungen, weil:

- Annahmen über TCO falsch sind
- Netzwerk- und Latenzanforderungen unterschätzt werden
- Governance nicht mitgedacht wird
- die internen Teams nicht alle Konsequenzen kennen
- Risiken in hybriden Modellen unsichtbar bleiben
- alte Systeme zu früh oder zu spät migriert werden

Ein strategischer Partner verhindert diese Fehler, indem er:

- die Gesamtarchitektur bewertet
- Workloads objektiv klassifiziert
- Risiken identifiziert, bevor sie entstehen
- die richtige Migrationsreihenfolge definiert
- Kostenmodelle neutral bewertet
- Zukunftsfähigkeit sicherstellt

„Die Wahl des falschen Betriebsmodells kostet im Mittelstand im Schnitt zwei Jahre Zeit und 20–40 % Mehrkosten.

Die Wahl des richtigen Modells schafft Planungssicherheit, und beschleunigt Digitalisierung messbar.“

Organisation, Rollen & Governance: Warum Strukturen wichtiger sind als Technik

Viele Cloud-Projekte scheitern nicht an Technik, Kosten oder der Wahl des Providers, sondern an fehlenden Rollen, unklaren Verantwortlichkeiten und einer zu spät etablierten Governance. Genau hier liegt der größte „Blind Spot“ mittelständischer Unternehmen. Die IT wird oft als rein technische Einheit verstanden, während Cloud eine strategische, organisatorische Transformation erfordert.

Cloud verändert alles:

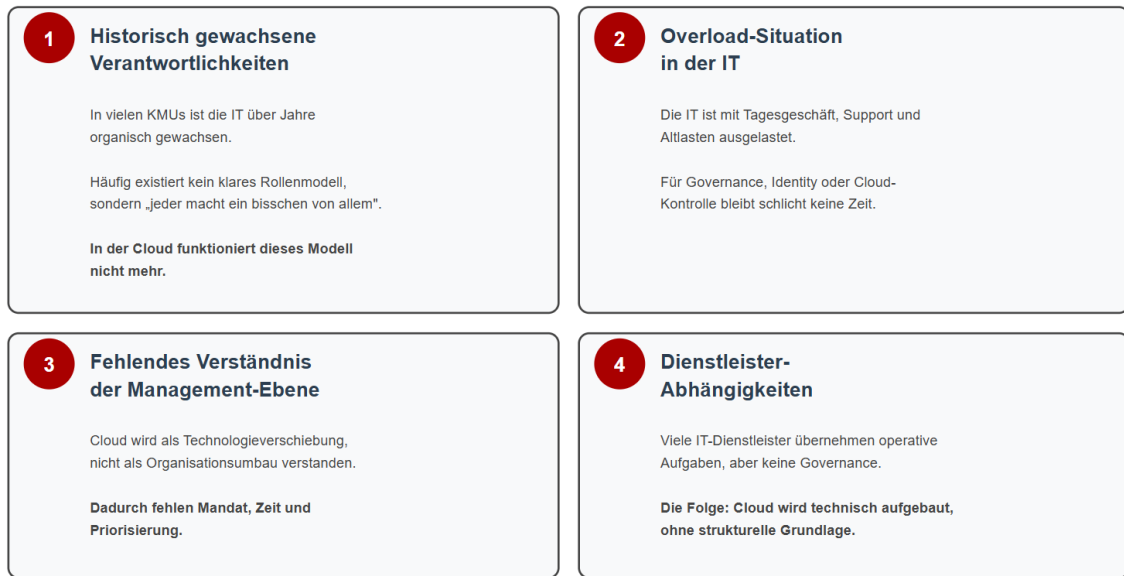
- wie Systeme bereitgestellt werden
- wie Berechtigungen funktionieren
- wie Kosten gemanagt werden
- wie Security gesteuert wird
- wie Entwicklungszyklen gestaltet sind
- wie Fachbereiche eingebunden werden
- wie Verantwortung verteilt ist

Unternehmen, die diese Veränderungen nicht bewusst gestalten, erleben unweigerlich Chaos, Kostenexplosionen oder Sicherheitsrisiken.

Cloud ist ein Organisationsprojekt — kein Infrastrukturprojekt.

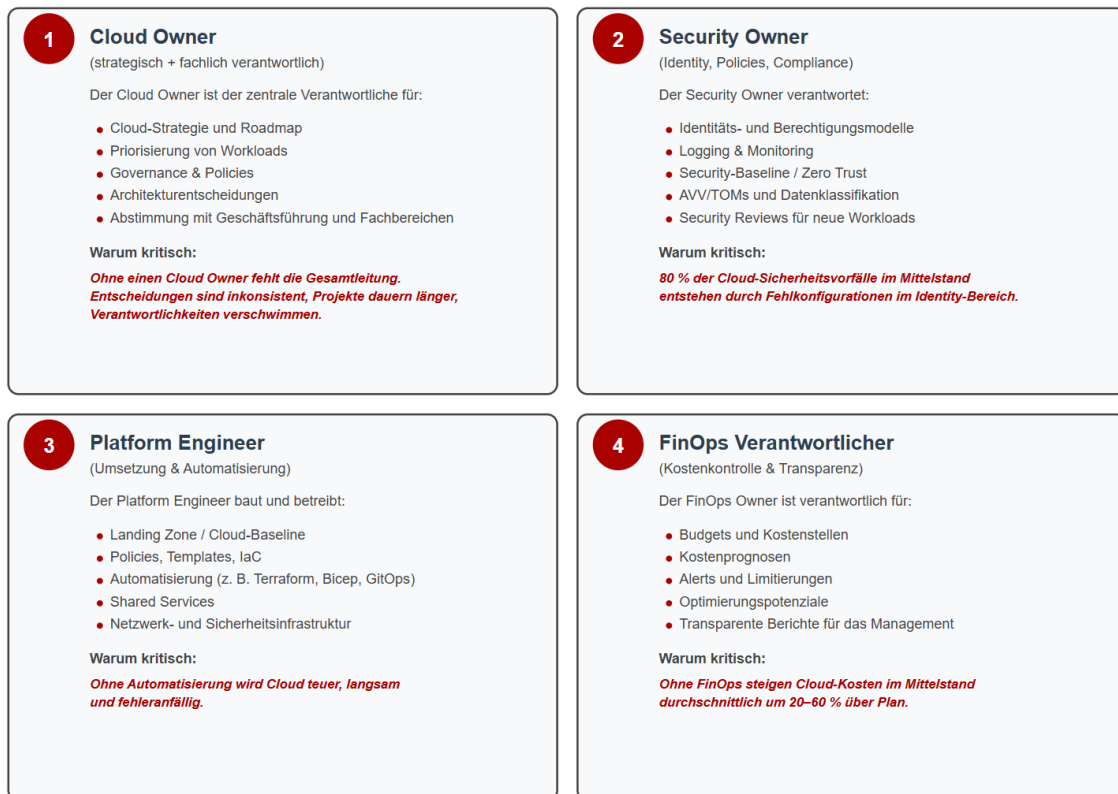
Warum Organisation & Governance im Mittelstand oft fehlen

Es gibt vier strukturelle Ursachen:



Vier unverzichtbare Rollen einer Cloud-Organisation

In jedem Unternehmen, egal ob 50 oder 500 Mitarbeitende, müssen mindestens vier Rollen klar definiert sein. Ohne diese Rollen entsteht Unklarheit und Risiko.



Governance: Der Ordnungsrahmen

Governance ist kein Handbuch, sondern ein Steuerungsmechanismus.

Für KMUs bedeutet das:

Essentielle Governance-Bausteine:

1. Naming Conventions
2. Tagging Standards (Owner, Cost Center, Environment, Criticality)
3. Identity & Access Policies
4. Kostenlimits und Budgets
5. Sicherheits-Policies (MFA, PIM, Logging)
6. Resource Lifecycle Management (Archivierung, Stilllegung)
7. Change- und Deployment-Regeln

Warum Governance früh kommen muss:

Wird Governance erst nach der Cloud-Einführung implementiert, entstehen:

- Chaos bei der Inventarisierung
- riesige Kostenaufwände für Refactoring
- Sicherheitsrisiken bei falsch konfigurierten Ressourcen

- Unklarheiten in Verantwortlichkeiten
- fehlende Auditfähigkeit
- Frust bei Fachbereichen

Regel:

Governance vor Deployment, nicht danach.

Handlungsempfehlungen für den Aufbau einer Cloud-Organisation

- Definieren Sie die vier Kernrollen klar und schriftlich.
- Stellen Sie sicher, dass jede Rolle ein Mandat und Entscheidungsbefugnis hat.
- Führen Sie monatliche Governance-Boards ein.
- Beginnen Sie mit einer minimalen, aber verbindlichen Governance-Baseline.
- Setzen Sie auf Automatisierung statt manuelle Prozesse.
- Stellen Sie sicher, dass Security und FinOps keine „Nebenjobs“ sind.
- Schulen Sie internes Personal gezielt („role-based enablement“).
- Dokumentieren Sie Policies in maximal 10 Seiten, nicht in 100.

Warum Sie Organisation & Governance nicht allein aufbauen sollten

Organisation ist das Gebiet, in dem interne Teams typischerweise die wenigste Erfahrung haben. Technik können viele, Governance können wenige.

Typische Fehler bei Eigenumsetzung:

- Rollen werden unklar oder gar nicht definiert
- Governance wird zu spät oder zu kompliziert aufgebaut
- Policies widersprechen sich oder werden nicht durchgesetzt
- SecOps und FinOps fehlen vollständig
- Fachbereiche erhalten zu spät Einbindung
- Identity-Architektur wird falsch geplant (fatal)
- Automatisierung wird zu gering priorisiert
- Verantwortlichkeiten überschneiden sich → Konflikte

Ein strategischer Partner:

- bringt praxiserprobte Rollenmodelle
- etabliert Governance in Wochen statt Monaten
- erkennt organisatorische Risiken früh
- moderiert zwischen Fachbereichen und IT
- verhindert übermäßige Komplexität
- stellt Entscheidungsfähigkeit sicher

„Es gibt keine erfolgreiche Cloud ohne klare Rollen.

Und es gibt keine klaren Rollen ohne klare Führung in der Einführungsphase.“

Vorgehensmodell: Die 4 Stufen zur Cloud-Strategie

Eine Cloud-Strategie ist kein IT-Projekt und kein Migrationsplan. Sie ist ein strukturierter Entscheidungsprozess, der aus Unsicherheit Klarheit und aus Komplexität eine nachvollziehbare Roadmap macht. Mittelständische Unternehmen, die ohne Methode starten, verlieren typischerweise 12–24 Monate durch Fehlentscheidungen, Überlastung der IT oder falsche Prioritäten. Unser Vorgehensmodell reduziert dieses Risiko drastisch und ermöglicht eine fundierte Strategie in **30–60 Tagen**, unabhängig davon, wie weit Ihr Unternehmen heute ist.

Die vier Stufen der erfolgreichen Cloud-Strategie

Stufe 1 – Zieldefinition & Erwartungsmanagement (1–2 Wochen)

„Falsche Ziele sind teurer als keine.“

Der größte Fehler vieler Cloud-Projekte liegt darin, dass Ziele implizit bleiben. Häufig hören wir Aussagen wie „Wir wollen moderner sein“, „Wir brauchen mehr Sicherheit“ oder „Die Hardware ist alt“. Das sind Ursachen, aber keine Strategziele.

Wir beginnen deshalb mit einem strukturierten Zielableitungsprozess, der folgende Fragen beantwortet:

- Welche Geschäftsprozesse sollen verbessert werden?
- Wo entstehen heute Verzögerungen, Risiken oder Kosten?
- Welche Workloads sind kritisch, welche sind ersetzbar?
- Welche regulatorischen Randbedingungen müssen erfüllt werden?
- Welche Risiken müssen reduziert werden (z. B. Security, Ausfall, CapEx)?
- Welche Innovationspotenziale bestehen?

Der Output ist ein messbarer Zielkatalog, z. B.:

- „Time-to-Provision von 5 Tagen auf 1 Tag reduzieren“
- „RPO von 24h auf 2h senken“
- „80 % aller privilegierten Zugriffe abgesichert“
- „20 % Kosteneinsparungen durch Automatisierung und PaaS“

Dieser Zielkatalog ist die Grundlage für jede weitere Entscheidung.

Warum Sie hier Unterstützung benötigen:

Interne Teams fokussieren auf das „Wie“. Wir stellen sicher, dass zuerst das „Warum“ sauber definiert ist, und verhindern damit falsch fokussierte Projekte.

Stufe 2 – Bewertung & Entscheidungsfindung (2–3 Wochen)

„Cloud ist kein Bauchgefühl.“

Diese Phase nutzt das 7-Dimensionen-Modell aus Kapitel 4, um Public, Hybrid und Private objektiv vergleichbar zu machen.

Arbeitsschritte:

1. Workload-Bestandsaufnahme (Inventar, Abhängigkeiten, Kritikalität)

2. Bewertung pro Dimension (Kosten, Sicherheit, Skalierbarkeit etc.)
3. Bewertung der Szenarien Public vs. Hybrid vs. Private
4. 5-Jahres-TCO-Modell
5. Risikoanalyse & Compliance-Betrachtung
6. Empfehlung der Zielarchitektur

Das Ergebnis ist ein klarer Entscheidungsreport, der dem Management eine faktenbasierte Wahl ermöglicht.

Warum Sie diese Phase nicht allein durchführen sollten:

Fehleinschätzungen führen zu Millionenprojekten, die nie Nutzen bringen. Ein strategischer Partner erkennt Risiken, interpretiert Kennzahlen richtig und stellt sicher, dass Entscheidungen belastbar sind.

Stufe 3 – Governance, Rollen & Cloud-Baseline (2 Wochen)

„Governance zuerst, Migration später.“

Bevor auch nur ein Workload bewegt wird, müssen folgende Grundlagen stehen:

- Rollenmodell (Cloud Owner, Security Owner, Platform Engineer, FinOps)
- Identity & Access Modell
- Naming & Tagging Standards
- Kostenlimits
- Logging & Monitoring
- Security Policies
- Backup-Strategie
- SLA-Definitionen
- Betriebskonzept (intern oder extern)

Wir erstellen in dieser Phase die sogenannte Cloud-Baseline / Landing Zone:

ein standardisiertes Fundament, das Security, Governance, Kostenkontrolle und Skalierbarkeit sicherstellt.

Warum Sie hier Unterstützung brauchen:

Eine falsch konfigurierte Identity- oder Governance-Struktur ist im Nachhinein kaum korrigierbar, und teuer.

Ein externer Partner baut eine stabile, zukunftsfähige Basis in Wochen statt Monaten.

Stufe 4 – Pilotierung & Roadmap (2–3 Wochen)

„Erste Erfolge schnell sichtbar machen.“

Der Pilot ist der kontrollierte Einstieg in den operativen Cloud-Betrieb. Er dient nicht primär als technische Übung, sondern als:

- Validierung der Governance
- Test des Betriebsmodells

- Identifikation organisatorischer Stolpersteine
- Schulungs- und Enablement-Maßnahme
- Quick Win zur Akzeptanzförderung

Typische Pilot-Workloads:

- interne Webapplikation
- DMS/Archivierung
- Test- und Entwicklungsumgebungen
- Reporting & Analytics
- Lastspitzen-Workloads

Parallel entsteht die 6–18-Monate-Roadmap, die beschreibt:

- Migrationsreihenfolge
- Modernisierungspotenziale
- Investitionsplanung
- Verantwortlichkeiten
- Ressourcenbedarf
- Erfolgskriterien (KPIs)

Warum ein Lighthouse-Pilot entscheidend ist:

Er schafft Vertrauen, Kompetenz und klare Linien, und verhindert Überraschungen in großen Projekten.

Der entscheidende Mehrwert eines Frühphasen-Partners

Viele Unternehmen versuchen, Cloud-Transformation intern zu initiieren und scheitern an denselben Punkten:

- Ziele sind unscharf oder widersprüchlich
- Governance kommt zu spät
- TCO wird falsch eingeschätzt
- Security wird nachträglich eingebaut
- Migration erfolgt ohne strategische Reihenfolge
- Fachbereiche werden zu spät eingebunden
- Verantwortlichkeiten sind diffus
- Partner kommen zu spät ins Spiel

Wir verhindern diese typischen Fehler durch:

- strukturierte Strategiearbeit
- klare Bewertung statt Bauchgefühl
- Erfahrung aus vielen Projekten
- professionelle Governance-Modelle
- enables It-Teams statt sie zu ersetzen
- Option zur Begleitung in Umsetzung & Betrieb, aber ohne Zwang

„Sie entscheiden, wie weit wir Sie begleiten.“

Wir sorgen dafür, dass die Basis stimmt, und Ihr Projekt erfolgreich wird.“

Case Studies: Drei typische Cloud-Ausgangslagen im Mittelstand

Cloud-Transformation ist nicht abstrakt. Sie zeigt sich in konkreten Situationen, typischen Mustern und wiederkehrenden Herausforderungen. In diesem Kapitel stellen wir drei realistische Szenarien dar, die häufig in Unternehmen zwischen 50 und 250 Mitarbeitenden auftreten. Die Beispiele sind fiktiv bewusst neutral formuliert, aber inhaltlich vollständig durch Erfahrungen aus Projekten belegt.

Case Study 1 – Produktionsbetrieb (85 Mitarbeitende)

Ausgangslage:

Ein mittelständischer Hersteller mit zwei Produktionsstandorten und einem kleinen IT-Team (3 Personen). Die IT-Landschaft besteht aus zwei ESXi-Hosts, einem SAN und 14 produktiven Workloads, davon vier eng mit Maschinen und Sensorik gekoppelt. Lastspitzen entstehen saisonal (Faktor 3).

Kein DevOps, geringe Automatisierung, Security teilweise implementiert (MFA ja, Logging nein).

Hauptprobleme:

- instabile Produktions-IT bei Peaks
- fehlende Elastizität
- ungeklärte Disaster-Recovery-Fähigkeit
- veraltete Hardware (EOL in 18 Monaten)
- stark ausgelastetes IT-Team

Bewertung im 7-Dimensionen-Modell:

- Kosten/TCO: 2 (Dauerlast + Maschinenkopplung + Lift&Shift wäre teuer)
- Sicherheit: 4
- Skalierbarkeit: 5
- Compliance: 4
- Agilität: 3
- Resilienz: 4
- Lock-in: **3**

Empfehlung: Hybrid Cloud

- Produktion & Maschinennähe On-Premises
- Business-Apps und Reporting in die Cloud
- DR in die Cloud verlagern
- Schrittweise Containerisierung prüfen

Wirkung:

- 80 % weniger Peak-bezogene Störungen
- deutlich höhere Resilienz
- niedrigere CapEx durch reduzierte On-Prem-Last
- stabile Grundlage für IIoT-Projekte

Warum der Kunde Unterstützung braucht:

Produktionsnahe Prozesse sind sensibel. Eine falsche Architekturentscheidung kann Maschinenstillstände verursachen. Ein strategischer Partner sorgt dafür, dass Cloud schrittweise, risikoarm und kompatibel zur OT/IT-Realität eingeführt wird.

Case Study 2 – Dienstleistungsunternehmen (120 Mitarbeitende)

Ausgangslage:

Ein B2B-Dienstleister mit hohem Remote-Anteil (20 % extern, 50 % mobil), bereits stark M365-zentriert. 90 % SaaS-Nutzung, vier lokale Anwendungen auf einem einzelnen Windows-Server ohne Redundanz. IT-Team: 4 Personen.

Digitalisierungsdruck sehr hoch, aber wenig Zeit.

Hauptprobleme:

- interne Prozesse dauern zu lange
- IT überlastet
- hohe Sicherheitsanforderungen durch Kunden
- fehlende Redundanz
- steigende Anforderungen an Governance

Bewertung im 7-Dimensionen-Modell:

- Kosten/TCO: 4
- Sicherheit: 4
- Skalierbarkeit: 4
- Compliance: 5
- Agilität: 5
- Resilienz: 4
- Lock-in: 3

Empfehlung: Public Cloud – Azure

- Ablösung On-Prem vollständig
- Entra ID als Identity-Zentrale
- Nutzung von PaaS-Angeboten (App Service, SQL PaaS, Storage)
- Einführung von CI/CD für interne Entwicklungen

Wirkung:

- Time-to-Provision von Wochen auf Stunden reduziert
- 30–40 % weniger Aufwand in Basisbetrieb
- deutlich erhöhte Transparenz im Security- und Compliance-Bereich
- neue Produkte schneller realisierbar

Warum der Kunde Unterstützung braucht:

Die größte Gefahr ist nicht Technik, sondern Aktionismus. Ein Cloud-Partner stellt sicher, dass nicht jede Fachabteilung „einfach drauflos klickt“, sondern klare Governance, Rollen und Prozesse etabliert werden, bevor Schatten-IT entsteht.

Case Study 3 – E-Commerce / Einzelhandel (60 Mitarbeitende)

Ausgangslage:

Ein lokales Einzelhandelsunternehmen mit wachsendem Online-Geschäft. Webshop On-Premises gehostet, häufig überlastet. Peak-Faktor 6 an Wochenenden/Events. IT-Team: 2 Personen. Keine Container, kein CI/CD, kein CDN, Backups manuell.

Hauptprobleme:

- Performance-Einbrüche im Shop
- keine Elastizität
- Betriebslast zu hoch für kleines IT-Team
- hohe Sicherheitsrisiken (manuelle Prozesse)
- unzureichende Backups

Bewertung im 7-Dimensionen-Modell:

- Kosten/TCO: 3 (Cloud kann günstiger oder leicht teurer sein, abhängig vom Architekturdesign)
- Sicherheit: 4
- Skalierbarkeit: 5
- Compliance: 4
- Agilität: 4
- Resilienz: 4
- Lock-in: 3

Empfehlung: Public Cloud + PaaS

- Webshop auf Azure App Service / Container Apps
- SQL-/PaaS-Datenbank
- CDN + DDoS-Schutz aktivieren
- CI/CD einführen

Wirkung:

- 90 % weniger Performance-Einbrüche
- massive Entlastung des IT-Teams
- schnelle Deployment-Zyklen
- sichere und skalierbare Architektur

Warum der Kunde Unterstützung braucht:

E-Commerce ist hochsensibel. Eine falsche Architektur führt zu Umsatzverlust oder Ausfallzeiten. Ein Partner sorgt dafür, dass Skalierung, Sicherheit, CI/CD und DR sauber implementiert sind, anstatt „nur die VM zu verschieben“.

Gemeinsame Muster aller drei Cases

1. Ohne Governance entstehen Chaos und Kostensteigerung.
2. Ohne Identity-Security steigt Risiko massiv.
3. Ohne Strategie werden falsche Workloads migriert.
4. Ohne klaren Fahrplan verzögern sich Projekte um Monate.

5. Ohne Partner werden Risiken falsch bewertet.

Gerade in KMUs fehlen Zeit, Ressourcen und Erfahrung, um diese Aspekte organisatorisch, technisch und wirtschaftlich zu beherrschen.

Beratungs-Mehrwert über alle Cases hinweg

„Unsere Stärke ist nicht, dass wir die Cloud bedienen können.

Unsere Stärke ist, dass wir Sie davor bewahren, die falsche Cloud-Entscheidung zu treffen und dafür sorgen, dass jede Cloud-Entscheidung wirtschaftlich, sicher und strategisch sinnvoll ist.“

Die größten Stolperfallen (und wie man sie vermeidet)

Die meisten fehlgeschlagenen Cloud-Projekte scheitern nicht an Technologie oder Tools, sondern an falschen Annahmen, fehlenden Strukturen und unzureichender Vorbereitung. In über 80 % der Fälle lassen sich die Ursachen auf wenige, wiederkehrende Muster zurückführen. Unternehmen verlieren dadurch Zeit, Geld und Vertrauen, oft ohne zu erkennen, wie vermeidbar diese Stolperfallen eigentlich gewesen wären.

Dieses Kapitel zeigt die größten Risiken, die Konsequenzen und vor allem:

Wie man sie verhindert.

Strategische & organisatorische Stolperfallen

Die häufigsten nicht-technischen Fehler bei Cloud-Migrationen

1 Cloud als Technikprojekt statt als strategische Entscheidung

Cloud betrifft: Organisation, Governance, Identity, Security, Kostenmodell, Betriebsprozesse und Fachbereiche.

Wenn der strategische Rahmen fehlt:

- falsche Priorisierung und hohe Kosten
- widersprüchliche Architekturentscheidungen
- unklare Verantwortlichkeiten

→ Klare, vom Management getragene Cloud-Strategie, basierend auf dem 7-Dimensionen-Modell.

2 Fehlende Governance

(zu spät, zu komplex oder gar nicht)

„Wir starten erst einmal, Governance kommt später.“
Das ist der sicherste Weg in Chaos.

Typische Folgen:

- Schatten-IT und Kostenexplosion
- Ressourcen ohne Besitzer
- widersprüchliche Konfigurationen

→ Governance als Startpunkt, nicht als Reaktion.
→ Minimal 8 Governance-Policies ab Tag 1.
→ Monatliches Cloud-Governance-Board.

3 Fachbereiche werden zu spät einbezogen

Cloud-Projekte scheitern, wenn Business und IT nicht gemeinsam steuern.

Folgen:

- fehlende Akzeptanz und Doppelarbeit
- hoher Abstimmungsaufwand
- ineffiziente Prozesse und Schattenprojekte

→ Fachbereiche früh in Zieldefinition einbinden.
→ Anforderungen strukturiert erfassen.
→ Pilotprojekte in enger Abstimmung durchführen.

4 Überforderung der internen IT

Wenn die IT zusätzlich zu Tagesgeschäft Cloud-Vorhaben stemmen soll, führt das zu:

Konsequenzen:

- Verzögerungen und hohe Fehleranfälligkeit
- unvollständige Umsetzung
- Sicherheitslücken und Burnout im Team

→ Rollen klar definieren.
→ Externe Unterstützung für Spitzenlast einplanen.
→ Automatisierung nutzen (IaC, CI/CD).

Technische & finanzielle Stolperfallen

Die häufigsten technischen und kostenbezogenen Fehler

5 „Lift & Shift“ ohne Modernisierung

„Erst mal heben wir alles in die Cloud – optimieren können wir später.“ In der Praxis passiert das nie.

Folgen:

- dauerhaft zu hohe Kosten
- schlechte Performance
- Sicherheitslücken in alten Anwendungen

→ Workloads priorisieren, modernisieren oder konsolidieren, bevor sie migriert werden.
→ Alternativen wie PaaS, Serverless oder SaaS prüfen.

6 Identity & Security werden unterschätzt

In der Cloud ist Identity der neue Perimeter.
Viele verfügen nicht über die notwendige Erfahrung in Entra ID, Conditional Access oder PIM.

Konsequenzen:

- unerkannte Sicherheitslücken
- Admin-Konten ohne Schutz

→ Zero-Trust-Prinzipien umsetzen (MFA, CA, PIM).
→ Logging und Monitoring aktivieren.
→ Security Owner früh einsetzen.

7 Kosten werden falsch eingeschätzt

Cloud ist nicht automatisch günstiger.
Ohne FinOps steigen Kosten typischerweise um 20–60 %.

Häufige Fehler:

- fehlendes Tagging und kein Right-Sizing
- keine Reservierungen
- unnötige Backups in Premium-Speicher

→ FinOps ab Woche 1 etablieren.
→ Kostenlimits in Subscription/Management-Group.
→ Regelmäßige Optimierung durch monatliche Reports.

8 Fehlender oder falscher Partner

Viele Dienstleister können Systeme betreiben – aber nicht strategisch bewerten oder transformieren.

Typische Risiken:

- Fokus auf Technik statt Strategie
- fehlende Governance-Kompetenz
- „Wir migrieren alles“-Mentalität

→ Partner wählen, die strategisch UND technisch denken.
→ Neutralität sicherstellen.
→ Erfahrung im Mittelstand prüfen.

Beratungs-Mehrwert: Der entscheidende Unterschied

Ein erfahrener strategischer Partner:

- verhindert die typischen Fehler aus 50+ Projekten
- bringt die Struktur, die intern fehlt
- sorgt für Klarheit in Strategie & Zielen
- erkennt Risiken bevor sie entstehen
- baut Governance und Identity korrekt auf
- schützt vor Kostenfallen
- entlastet das interne Team
- stellt sicher, dass Cloud ein unternehmerischer Vorteil wird

„Cloud scheitert nicht an fehlender Technik. Cloud scheitert daran, dass Unternehmen ohne Kompass starten.

Unser Job ist es, dieser Kompass zu sein.“

Handlungsempfehlungen in drei Transformationsphasen

Eine erfolgreiche Cloud-Transformation entsteht nicht durch einen großen Sprung, sondern durch ein strukturiertes, kontrolliertes Vorgehen in klar definierten Phasen. Jede Phase baut auf der vorherigen auf, schärft die Entscheidungsgrundlage und reduziert Risiken. Die Reihenfolge ist entscheidend, nicht die Geschwindigkeit.

Viele Projekte scheitern, weil Firmen die Phasen überspringen oder vermischen: Governance wird nachträglich eingeführt, Security später „nachgezogen“, Fachbereiche erst beim Rollout einbezogen. Das Ergebnis ist Chaos, Kostenexplosion oder Sicherheitsprobleme.

Das folgende Modell beschreibt **drei robuste Transformationsphasen**, die sich in allen erfolgreich umgesetzten Cloud-Projekten wiederfinden.

1 Orientierung & Fundament

Klarheit schaffen

Zentrale Arbeitspakete:

- **Zieldefinition & Erwartungsmanagement**
Messbare Ziele mit Geschäftsführung, IT und Fachbereichen entwickeln
- **Bewertung mit dem 7-Dimensionen-Modell**
Public, Hybrid und Private objektiv vergleichen; Workloads kategorisieren
- **Governance-Definition**
Mindestens 8 Policies: Identity, Security, Tagging, Cost Management, etc.

OUTPUT PHASE 1:

- ✓ Zielbild ✓ Entscheidungsmodell ✓ Governance-Basis
- ✓ Risikoanalyse ✓ Workload-Klassifikation



2 Struktur & Befähigung

Die Grundlage für sicheren Cloud-Betrieb

Zentrale Arbeitspakete:

- **Rollen & Verantwortlichkeiten**
Die vier kritischen Rollen werden besetzt und formalisiert
- **Identity & Security Baseline**
MFA, Conditional Access, Logging, PIM und Backup-Härtung aktivieren
- **Aufbau der Cloud-Baseline / Landing Zone**
Netzwerk, Subscriptions, Policies, Monitoring, Automatisierung, Kostenlimits
- **Fachbereichseinbindung**
Anwendungsfälle priorisieren, Erwartungen abstimmen, Prozesse neu denken

OUTPUT PHASE 2:

- ✓ Vollständige Cloud-Baseline ✓ Identity- und Security-Fundament ✓ Governance implementiert
- ✓ Rollen aktiv ✓ Unternehmensweite Klarheit über Vorgehen



3 Umsetzung & Skalierung

Vom Pilot zur Roadmap

Zentrale Arbeitspakete:

- **Pilot-Workload**
Validierung: Governance, Security, Architektur und Prozess-/Skill-Gaps identifizieren
Typische Kandidaten: interne Webanwendung, Reportings, Testumgebungen
- **Organisations- & Betriebsmodell testen**
Verantwortlichkeitslücken, Skill-Bedarfe und Optimierungspotenziale identifizieren
- **Roadmap und Migrationsplan**
Basierend auf Pilot-Erkenntnissen: Migration, Modernisierung, Automatisierung, FinOps-Etablierung, Security-Reifeentwicklung und Betriebsmodell

OUTPUT PHASE 3:

- ✓ Validiertes Betriebsmodell ✓ Roadmap 6–18 Monate ✓ Migrationsreihenfolge
- ✓ Klare Verantwortlichkeiten ✓ Laufende Optimierungszyklen

Warum diese drei Phasen entscheidend sind

Unternehmen, die ohne klare Struktur starten, schaffen sich:

- Governance-Schulden
- technische Schulden
- Sicherheitsrisiken
- unnötige Kosten
- Frustration im Team
- Verzögerungen von 12–24 Monaten

Unternehmen, die nach diesem Modell arbeiten, erreichen:

- schnelle Klarheit
- kalkulierbare Kosten
- hohe Akzeptanz
- minimales Risiko
- effiziente Umsetzung
- nachhaltige Betriebssicherheit

Beratungs-Mehrwert: Warum ein externer Partner die Transformation beschleunigt

Ein erfahrener strategischer Partner sorgt für:

- einen sauberen Start
- realistische Zielsetzung
- objektive Bewertung
- vollständige Governance
- konsistente Identity- und Security-Architekturen
- klare Verantwortlichkeiten
- professionelle Moderation zwischen IT und Fachbereichen
- schnellere Entscheidungsfindung
- schnellere Pilot-Ergebnisse
- nachhaltig stabile Cloud-Strukturen

*„Die drei Phasen der Cloud-Transformation lassen sich allein durchlaufen,
aber mit einem erfahrenen Partner werden sie schneller, sicherer und wirtschaftlich erfolgreicher.“*

Warum Sie diese Reise nicht allein machen sollten

Cloud-Transformation ist kein rein technisches Vorhaben. Sie betrifft Strategie, Organisation, Sicherheit, Prozesse, Kosten, Architektur und die gesamte IT- und Unternehmensentwicklung. Genau deshalb scheitern viele mittelständische Unternehmen nicht an Tools oder Technologie, sondern daran, dass sie die Komplexität unterschätzen und die Transformation allein stemmen wollen.

Dieses Kapitel zeigt, warum ein externer strategischer Partner nicht „nice to have“ ist, sondern ein entscheidender Erfolgsfaktor, wenn Cloud-Entscheidungen dauerhaft zu besseren Ergebnissen führen sollen.

Cloud ist ein Erfahrungsprojekt, kein Lernprojekt

Interne IT-Teams sind fachlich stark und leisten Erstaunliches im Tagesgeschäft.

Doch Cloud-Transformation ist ein Gebiet, das man nicht nebenbei lernen kann.

Warum?

- es ist ein komplexes Architekturthema
- ein Sicherheitsprojekt
- ein Organisationsumbau
- ein Betriebsmodellwechsel
- ein Compliance-Projekt
- ein finanzielles Steuerungsmodell (FinOps)
- und ein Change-Prozess mit fachlicher, technischer und kultureller Dimension

Damit ist Cloud kein Projekt, das „Learning by Doing“ erlaubt.

Fehler sind teuer, riskant und schwer reversibel.

Ein erfahrener Partner bringt fertige Modelle, Vorlagen, Entscheidungslogiken und Best Practices, die intern erst über viele Jahre aufgebaut werden könnten.

Die größten Risiken bei Alleingang

Unternehmen, die allein starten, laufen fast immer in dieselben Risiken:

1

Fehlende Governance

Führt zu Kostenexplosion, Inkonsistenzen, Schatten-IT und manuellem Wildwuchs.

2

Fehler in der Identity-Architektur

Der größte Sicherheitshebel – falsche Konfigurationen sind gefährlich und kaum sichtbar.

3

Kosten werden massiv unterschätzt

Ohne FinOps steigen Cloud-Kosten erfahrungsgemäß um 20–60 %.

4

Workloads werden falsch priorisiert

„Wir nehmen alles oder das Falsche mit“ führt zu jahrelangen Rückständen.

5

Migration ohne Modernisierung

Erzeugt neue technische Schulden statt sie abzubauen.

6

Interne Überlastung

Cloud kommt oben auf die ohnehin vollen Aufgaben. Teams geraten in Burnout-Zonen.

7

Fehlender strategischer Blick

Teams fokussieren Technik. Doch Cloud ist vor allem Organisation und Betriebsmodell.

Ohne externen Partner sind diese Risiken real –
und sie summieren sich.

Was ein strategischer Partner wirklich leistet

Es geht nicht darum, Arbeit „abzunehmen“.

Es geht darum, Risiken vorab zu eliminieren, Entscheidungen klarzumachen und Strukturen aufzubauen, auf denen IT und Business langfristig erfolgreich sein können.

Ein guter Cloud-Strategiepartner bringt:

- 1 Klarheit**
Wir helfen dabei, Ziele präzise zu definieren, Prioritäten zu setzen und Entscheidungsfähigkeit zu schaffen.
- 2 Objektivität**
Wir sind nicht gebunden an bestehende Infrastruktur oder „heilige Kühe“. Wir bewerten neutral.
- 3 Struktur & Modelle**
Fertige Frameworks, Rollenmodelle, Betriebsmodelle, Governance-Bausteine und TCO-Vorlagen.
- 4 Risiko-Reduktion**
Wir verhindern Fehlentscheidungen, bevor sie entstehen – nicht danach.
- 5 Geschwindigkeit**
Was intern Monate dauert, lässt sich mit unserem Vorgehensmodell in wenigen Wochen realisieren.
- 6 Know-how-Transfer**
Wir befähigen Ihre Teams – wir ersetzen sie nicht.
- 7 Kontinuität**
Wir unterstützen auf Wunsch auch beim Aufbau von Betrieb, FinOps, Security oder Automatisierung.

Warum frühe Einbindung entscheidend ist

Die größten Fehler entstehen immer zu Beginn:

- Ziele unklar
- falsche Annahmen
- fehlende Governance
- Identity-Fehlentscheidungen
- Workload-Priorisierung ohne Systematik
- Kosten werden nachträglich optimiert statt vornherein geplant

Wird ein Partner erst spät eingebunden, ist der Schaden oft schon entstanden:

- Governance muss aufwendig korrigiert werden

- Identity-Strukturen müssen neu aufgebaut werden
- Migrationen müssen rückgängig gemacht werden
- Kosten laufen aus dem Ruder
- Frustration entsteht im Team

Frühe strategische Begleitung spart Zeit, Kosten und Risiko.

Kontrolle behalten, ohne Abhängigkeit

Eine gute Beratung macht Sie nicht abhängig. Sie macht Sie fähig.

Deshalb verfolgen wir einen Ansatz, der neutral, unabhängig und flexibel ist:

- Sie können nach der Strategie selbst umsetzen
- oder mit Ihrem IT-Dienstleister
- oder mit uns
- oder in Kombination

Wir schaffen die Grundlagen, damit jede dieser Optionen funktioniert. Kein Lock-in, keine versteckten Abhängigkeiten, keine „Techniker-only“-Lösungen.

Die Kernbotschaft

„Sie können die Cloud technisch allein betreiben. Aber Sie können die Cloud nicht allein strategisch richtig entscheiden.“

Wir setzen genau dort an bevor Fehler entstehen. Und wir begleiten Sie nur so weit, wie Sie es wirklich wollen.

Unser Beratungsansatz & der Mehrwert für Ihr Unternehmen

Eine Cloud-Transformation ist ein komplexes Vorhaben mit strategischer, technischer, organisatorischer und kultureller Dimension. Die meisten Beratungen setzen erst ein, wenn die technische Umsetzung beginnt. Unsere Erfahrung zeigt jedoch:

Die entscheidenden Weichen werden viel früher in der Strategiephase gestellt. Und genau dort setzen wir an.

Unser Beratungsansatz ist so aufgebaut, dass er Unternehmen im Mittelstand befähigt, informierte, nachhaltige und risikoarme Entscheidungen zu treffen. Ohne Abhängigkeit, ohne Hype, ohne unnötige Komplexität.

Unser Grundprinzip: Strategie vor Migration

Viele Dienstleister beginnen sofort mit technischen Entscheidungen:

Welche VMs? Welche Subscriptions? Welche Tools?

Wir tun das Gegenteil. Wir beginnen mit:

- Zielen
- Prozessen
- Organisation
- Sicherheit
- Governance
- Wirtschaftlichkeit
- Prioritäten
- Workload-Bewertung

Die Technik folgt erst danach: eindeutig, nachvollziehbar und auf Basis klarer Kriterien.

Ihr Vorteil: Jede Entscheidung ist begründet, dokumentiert und langfristig tragfähig.

Unser Vorgehen: Struktur statt Bauchgefühl

Unser Ansatz basiert auf einem methodisch klaren Framework, das bereits bei zahlreichen mittelständischen Projekten erfolgreich eingesetzt wurde:

1 Strategische Zielidentifikation

Gemeinsam mit Geschäftsführung, IT und Fachbereichen definieren wir messbare Ziele – nicht nur technische, sondern organisatorische und wirtschaftliche.

2 Objektive Bewertung mit dem 7-Dimensionen-Modell

Wir bewerten Public, Hybrid und Private Cloud entlang eines transparenten Scoring-Modells. Kein Bauchgefühl, keine Marketingversprechen, sondern klare Bewertungslogik.

3 Governance & Rollenmodell

Wir etablieren die Struktur, die Cloud möglich macht: Cloud Owner, Security Owner, Platform Engineer, FinOps. Plus verbindliche Policies für Identity, Security, Kosten, Betrieb und Architektur.

4 Architektur- & Betriebsdesign

Wir entwickeln eine skalierbare, sichere und wirtschaftliche Zielarchitektur (Landing Zone, Netzwerk, Identity, Monitoring, Backup, PaaS-Strategie).

5 Lighthouse-Pilot & Roadmap

Wir begleiten einen ersten Pilot, validieren Governance, Sicherheit und Betriebsmodell und erstellen eine Roadmap für 6–18 Monate.

Und das Wichtigste:

Sie entscheiden, wie weit wir Sie begleiten — von der Strategie bis hin zu Betrieb und Weiterentwicklung.

Was uns von klassischen Dienstleistern unterscheidet

Viele IT-Dienstleister und Systemhäuser arbeiten umsetzungsorientiert.

Wir arbeiten entscheidungsorientiert.

Das bedeutet konkret:

1

Wir sind unabhängig von Technologie und Providern

Wir verkaufen keine Software, keine Lizenzen, keine Hardware. Wir beraten neutral.

2

Unsere Perspektive ist strategisch, nicht operativ-technisch

Wir denken in Wertbeiträgen, Risiken, Wirtschaftlichkeit und Reifegrad — nicht nur in Ressourcen und Workloads.

3

Wir verhindern Fehlentscheidungen frühzeitig

Fehler, die nachträglich Millionen kosten können, werden von uns bereits in der Strategiestufe erkannt und ausgeschlossen.

4

Wir bauen Strukturen, die Bestand haben

Role-based Modelle, Governance, Identity-Architektur, FinOps — das sind tragende Elemente für die nächsten 10 Jahre.

5

Wir befähigen Ihre IT-Teams statt sie zu ersetzen

Enablement, Coaching und Wissenstransfer sind zentrale Bestandteile unseres Ansatzes.

6

Wir bleiben flexibel

Sie können:

- selbst umsetzen
- mit Ihrem bestehenden IT-Dienstleister arbeiten
- oder uns für Tiefthemen hinzuziehen

Kein Lock-in. Keine Zwangsbegleitung. Kein Upselling.

Der konkrete Mehrwert für Ihr Unternehmen

Unsere Beratung sorgt dafür, dass:

- Sie Cloud-Entscheidungen treffen, die wirtschaftlich sinnvoll sind
- Ihre IT weniger Betriebslast hat
- Ihre Sicherheitsrisiken drastisch sinken
- Ihre Kosten plan- und steuerbar bleiben
- Sie intern schneller innovieren können
- Sie eine Governance-Struktur erhalten, die geprüft und tragfähig ist
- Ihre Fachbereiche eingebunden und unterstützt werden
- Ihre Migration risikoarm und fokussiert verläuft

- Sie langfristig unabhängig und kompetent werden

Mit uns gewinnen Sie Geschwindigkeit, Klarheit und Risikokontrolle.

Unser Leistungsversprechen

Wir begleiten Sie genau so weit, wie Sie es wollen:

- Nur Strategie?
Perfekt. Das ist unser Kerngeschäft.
- Strategie + Pilot?
Sehr gern, wir unterstützen wo nötig.
- Strategie + Umsetzung + Betrieb?
Möglich, aber nicht verpflichtend.
- Wissenstransfer & Enablement?
Bestandteil jedes Projekts.

Unser Ziel ist nicht, Sie zu binden, sondern Sie stark zu machen.

Unser abschließendes Commitment

„Wir stellen sicher, dass jede Cloud-Entscheidung einen klaren geschäftlichen Nutzen hat, und dass Ihre Organisation bereit ist, diesen Nutzen nachhaltig umzusetzen.“

Mit diesem Beratungsansatz ermöglichen wir mittelständischen Unternehmen eine sichere, wirtschaftliche und moderne Cloud-Strategie, die nicht nur heute funktioniert, sondern in den nächsten Jahren Bestand hat.