
WHITEPAPER · TRANSFORMATION & CLOUD

Cloud Transformation und Technology Migration

HERAUSGEBER

Manuel Fernandez

VERÖFFENTLICHT

15. Oktober 2026

01 Executive Summary

Eine Cloud-Migration ist kein Umzug von Servern, sondern die Einführung eines neuen Betriebsmodells. Wer Workloads verlagert, ohne Verantwortlichkeiten, Plattformgrundlagen, Kostensteuerung und Sicherheitsregeln festzulegen, verlagert die bestehenden Probleme – und fügt neue hinzu.

Dieses Whitepaper beschreibt einen strukturierten Weg von der Bestandsaufnahme bis zum Regelbetrieb: Workload-Assessment, Zielbetriebsmodell und Landing Zone, eine Entscheidung je Workload entlang der branchenüblichen „7 R“, Wellenplanung, Cutover mit Rollback-Kriterien sowie Hypercare und formale Übergabe. Querschnittlich laufen Kosten-Governance (FinOps), Sicherheit und Datenresidenz. Die Kernaussage: Über den Erfolg entscheiden die Vorarbeiten – Inventar, Abhängigkeiten, Zielplattform, Verantwortungsmodell – und die Disziplin in der Übergabe, weniger die Migration einzelner Workloads. Entscheidungsträger sollten daher früh in diese Grundlagen investieren und die Migrationsgeschwindigkeit erst erhöhen, wenn Plattform und Abläufe in einer Pilotwelle erprobt sind.

Zielgruppe sind IT-Leitung, Enterprise- und Cloud-Architekten, Programm- und Projektleitungen sowie Verantwortliche für Betrieb, Informationssicherheit und Controlling. Ergänzend empfehlen wir das DIP-Whitepaper „Technology Refresh und Migrationsmanagement“: Es behandelt die vorgelagerte Frage, wann eine Migration sinnvoll ist und welche Migrationstypen es gibt. Das vorliegende Dokument setzt dort an, wo die Cloud als Zielumgebung feststeht oder geprüft wird.

02 Problemstellung

Die NIST-Definition (SP 800-145) beschreibt Cloud Computing über fünf Merkmale: bedarfsgesteuerte Selbstbedienung, breiter Netzwerkzugang, Ressourcen-Pooling, schnelle Elastizität und gemessene Nutzung. Genau diese Merkmale verändern, wie IT organisiert, abgerechnet und abgesichert werden muss. Wer sie nur als neue Infrastruktur behandelt, unterschätzt den organisatorischen Teil der Veränderung. Typische Schwierigkeiten:

- **Unvollständiges Bild der Ausgangslage:** Inventare sind lückenhaft; Schnittstellen, Batch-Ketten, fest verdrahtete Adressen oder Lizenzbindungen werden erst während der Migration entdeckt und verschieben Termine.
- **Fehlendes Zielbetriebsmodell:** Das Modell der geteilten Verantwortung (Shared Responsibility) verschiebt Zuständigkeiten je nach IaaS, PaaS oder SaaS. Ungeklärt entstehen Lücken oder Doppelarbeit bei Plattform, Identitäten, Patching und Backup.
- **Plattform ohne Leitplanken:** Erste Workloads in unstrukturierten Konten führen zu uneinheitlichen Netzwerk- und Berechtigungsmustern, deren spätere Konsolidierung aufwendig ist.

- **Unklare Kostenwirkung:** Nutzungsabhängige Abrechnung verlagert Kostenentscheidungen in viele technische Einzelentscheidungen. Ein Business Case ohne Parallelbetrieb, Migrationsaufwand und Schulung greift zu kurz.
- **Regulatorik und Datenresidenz:** Vorgaben zu Speicherort, Zugriff, Verschlüsselung und Auslagerung – bei personenbezogenen Daten einschließlich der DSGVO-Regeln zur Drittlandübermittlung – prägen Regionswahl und Architektur und lassen sich nicht am Projektende „nachprüfen“.

03 Vorgehen und Phasen

Das Vorgehen folgt der Logik, die auch die Cloud-Adoption-Frameworks der großen Anbieter beschreiben, ist aber anbieterneutral formuliert. DIP begleitet solche Vorhaben von der Initialanalyse des Unternehmens, der Technologieumgebung und der regulatorischen Anforderungen über die Koordination der ausführenden Teams bis zur technischen Unterstützung in der Umsetzung und zur Dokumentation.

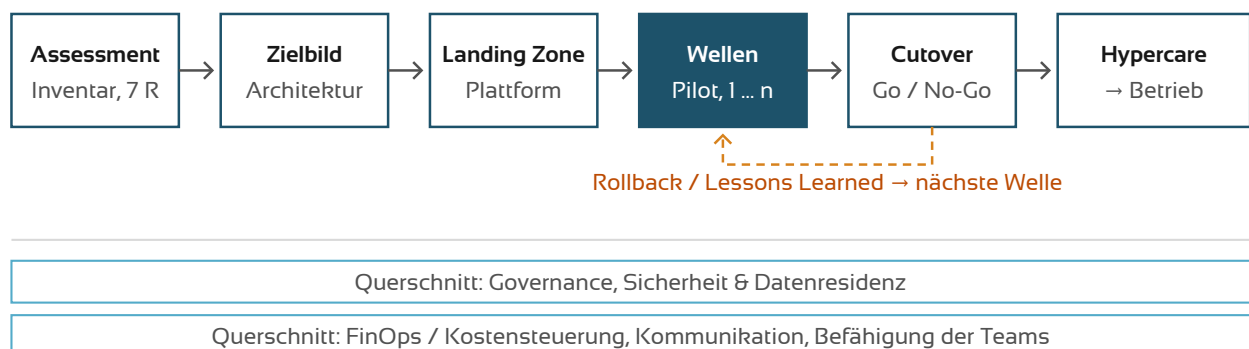


Abbildung 1: Phasenmodell einer Cloud-Transformation mit Rückkopplung aus jedem Cutover in die Wellenplanung und durchgehenden Querschnittsthemen.

01 Strategie und Entscheidungskriterien

Ziele klären – etwa schnellere Bereitstellung, Ablösung eines Rechenzentrumsvertrags, Modernisierung, Resilienz – und daraus Kriterien ableiten, nach denen jeder Workload bewertet wird: Kosten, Termin, Risiko, Modernisierungsgrad, Regulatorik. Die Gewichtung wird mit dem Management abgestimmt und dokumentiert, ebenso der Plattformansatz (ein Anbieter, mehrere Anbieter oder hybrid).

02 Workload-Assessment

Jeder Workload wird nach einem einheitlichen Raster erfasst: Kritikalität und Wiederanlaufziele (RTO/RPO), technische Merkmale und Lastprofil, Abhängigkeiten, Lizenzbedingungen, Datenklassifikation und regulatorische Vorgaben sowie

Verantwortliche. Discovery-Werkzeuge liefern Auslastungs- und Verbindungsdaten; Interviews mit Anwendungsverantwortlichen machen fachliche Abhängigkeiten sichtbar. Ergebnis ist je Workload eine Strategie nach den „7 R“ (Abschnitt 04) mit Aufwands- und Risikoeinschätzung.

03 Zielbetriebsmodell und Landing Zone

Das Zielbetriebsmodell legt fest, wer was verantwortet: ein Plattformteam bzw. Cloud Center of Excellence für Standards und Automatisierung, Anwendungsteams für ihre Workloads, Sicherheit, Betrieb und Controlling mit klaren Schnittstellen und angepassten ITSM-Prozessen. Die Landing Zone ist die vorbereitete Zielumgebung mit Leitplanken: Konto- bzw. Abonnement-Hierarchie, Identitäten und Rollen, Netzwerkgrundstruktur, zentrale Protokollierung, Richtlinien für Regionen und Dienste, Schlüsselverwaltung, Tagging und Budgets – als Code beschrieben und versioniert. Als Prüfmaßstab für die Zielarchitektur eignen sich die Well-Architected-Frameworks der Anbieter.

04 Wellenplanung

Workloads werden nach Abhängigkeiten (eng gekoppelte Systeme gemeinsam), Risiko (repräsentative, weniger kritische zuerst), Terminen (Vertrags- und Supportenden, Geschäftsspitzen) und Teamkapazität zu Wellen gebündelt. Eine Pilotwelle erprobt Werkzeuge, Runbooks und Zusammenarbeit. Jede Welle hat Umfang, Zeitplan, Verantwortliche und Eingangskriterien – etwa abgeschlossene Abhängigkeitsanalyse, bereitgestellte Zielumgebung und ein mit den Fachbereichen abgestimmtes Testkonzept. Erkenntnisse aus jeder Welle fließen in die Planung der folgenden ein; der Wellenplan ist damit ein lebendes Steuerungsinstrument, kein einmal beschlossener Zeitplan.

05 Migration, Test und Cutover

Je Workload: Zielumgebung bereitstellen, Daten replizieren, Anwendung übertragen, technisch und fachlich testen. Der Engpass ist meist die Koordination zwischen Plattform-, Anwendungs-, Netzwerk- und Sicherheitsteams, Fachbereichen und Dienstleistern. Der Cutover folgt einem geprüften Runbook; vorab entscheidet ein formales Go/No-Go anhand vereinbarter Kriterien. Festgelegt sind außerdem Rollback-Kriterien, ein „Point of no Return“ und der Umgang mit zwischenzeitlich geschriebenen Daten.

06 Hypercare und Betriebsübergabe

Nach dem Cutover bleibt das Migrationsteam für eine vorab definierte Zeit verfügbar; Störungen, Monitoring und Kostenentwicklung werden eng beobachtet. Endkriterien sind etwa störungsfreie Geschäfts- oder Batch-Zyklen und abgearbeitete offene Punkte. Die Übergabe an den Regelbetrieb ist ein formaler Schritt mit Abnahme von Betriebshandbuch, Monitoring, Backup-Tests, Berechtigungen, Kostenzuordnung und Eskalationswegen. Der

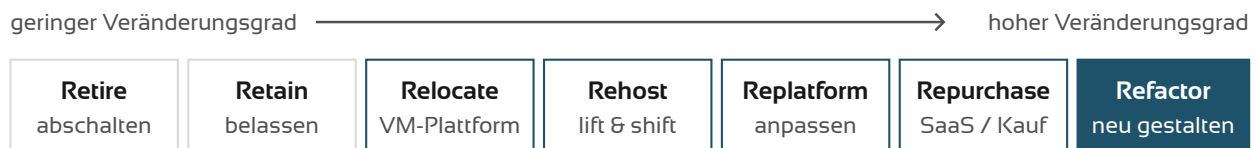
Betrieb bestätigt die Übernahme schriftlich; offene Punkte werden mit Verantwortlichen und Terminen übergeben, statt stillschweigend im Projekt zu verbleiben.

07 Stilllegung und Abschluss

Erst nach der Übergabe wird die Altumgebung stillgelegt: Daten archiviert oder gelöscht, Lizenzen und Verträge gekündigt, Netzwerkfreigaben entfernt. Ein Abschlussbericht je Welle hält Ergebnisse, Abweichungen und Lessons Learned fest, die in die nächste Welle einfließen.

04 Migrationsstrategien je Workload: die „7 R“

Für die Entscheidung je Workload hat sich eine Systematik etabliert, die ursprünglich mit fünf, inzwischen meist mit sieben „R“ beschrieben wird. Sie ist eine Branchenkonvention, kein Standard; Bezeichnungen variieren je nach Quelle. Entscheidend ist, dass jede Zuordnung bewusst getroffen und begründet wird.



Typische Leitfragen im Assessment

- 1 Wird der Workload fachlich noch benötigt? → sonst Retire
- 2 Spricht vorerst etwas gegen die Verlagerung (Regulatorik, Ablösung)? → Retain
- 3 Existiert eine geeignete Standardlösung als Service? → Repurchase
- 4 Rechtfertigt der Geschäftsnutzen eine Neugestaltung? → Refactor, sonst Replatform
- 5 Ist Zeit der dominierende Faktor? → Rehost oder Relocate, Modernisierung später

Abbildung 2: Die „7 R“ als Branchenkonvention, geordnet nach Veränderungsgrad, mit vereinfachten Leitfragen. Die Reihenfolge der Fragen ist ein Vorschlag, keine feste Entscheidungslogik.

- **Retire:** abschalten statt migrieren.
- **Retain:** vorerst bewusst belassen, z. B. wegen Regulatorik oder geplanter Ablösung.
- **Relocate:** ganze Virtualisierungs- oder Container-Plattform verlagern, ohne Systeme umzubauen.
- **Rehost:** Server weitgehend unverändert übertragen; schnell, nutzt Cloud-Eigenschaften aber kaum.
- **Replatform:** gezielte Anpassungen, etwa Wechsel auf einen verwalteten Datenbankdienst.
- **Repurchase:** Ablösung durch ein Standardprodukt, häufig SaaS.
- **Refactor:** Neugestaltung zur vollen Nutzung von Plattformdiensten; höchster Aufwand.

Strategien werden oft kombiniert: zunächst Rehost, um einen Termin zu halten, später Replatform oder Refactor. Diese zweite Stufe gehört von Anfang an in Wellenplan und Budget – sonst bleibt das Provisorium dauerhaft. Umgekehrt ist nicht jeder Workload ein Kandidat für Refactor: Wo der fachliche Nutzen eine Neugestaltung nicht trägt, ist eine schlichte, gut betriebene Lösung oft die wirtschaftlichere Wahl.

HYPOTHETISCHES BEISPIEL

Ein Auftragsportal mit eigener Datenbank, zwei Batch-Schnittstellen zum ERP-System und einem Dateiaustausch mit einem Logistikpartner wird bewertet. Das Portal wird weiter benötigt, eine Standardlösung ist nicht vorgesehen, der Rechenzentrumsvertrag läuft aus. Entscheidung: Rehost in einer frühen Welle gemeinsam mit den Batch-Schnittstellen, um Latenzprobleme zu vermeiden; Replatform der Datenbank in einer späteren Welle. Der Partneraustausch wird als eigenes Risiko geführt, weil sich Quell-IP-Adressen ändern und der Partner Freigaben anpassen muss.

05 Querschnittsthemen

FinOps und Kosten-Governance

Die FinOps Foundation beschreibt FinOps als gemeinsame Kostenverantwortung von Technik, Finanzen und Fachbereichen und gliedert die Arbeit in die Phasen „Inform“, „Optimize“ und „Operate“. Für die Migration heißt das:

- Tagging und Kontenstruktur so festlegen und per Richtlinie durchsetzen, dass jede Ressource Workload, Kostenstelle und Verantwortlichem zugeordnet ist.
- Budgets und Warnschwellen je Welle einrichten; Kostenberichte gehören in die Hypercare.
- Parallelbetrieb im Business Case einplanen und die Stilllegung terminieren.
- Größen und Laufzeitbindungen erst festlegen, wenn Lastprofile in der Cloud belastbar bekannt sind.

Sicherheit, Datenschutz und Datenresidenz

Sicherheit wird in der Landing Zone verankert, nicht je Workload neu erfunden: Berechtigungen nach minimalen Rechten, Mehr-Faktor-Authentifizierung für privilegierte Zugänge, Verschlüsselung mit geregelter Schlüsselverwaltung, zentrale Protokollierung, laufende Konfigurationsprüfung und ein auf die Cloud erweitertes Patchmanagement. Die Shared-Responsibility-Zuordnung wird je genutztem Dienst dokumentiert.

Aus der Datenklassifikation folgt, welche Daten in welchen Regionen liegen und wer zugreifen darf. Zu prüfen sind Regionswahl, Support- und Administrationszugriffe des Anbieters, Schlüsselhoheit, Auftragsverarbeitung und Drittlandübermittlung nach DSGVO sowie branchenspezifisches Auslagerungsmanagement. Der BSI-Kriterienkatalog C5 bietet eine in Deutschland verbreitete Grundlage, um Cloud-Dienste anhand von Prüfberichten zu bewerten; die dort beschriebenen ergänzenden Kundenkontrollen bleiben Teil des eigenen Sicherheitskonzepts. Die rechtliche Einzelfallbewertung gehört zu den zuständigen Fachleuten.

Befähigung und Kommunikation

Cloud-Betrieb verlangt andere Fähigkeiten als klassischer Rechenzentrumsbetrieb: Infrastruktur als Code, Automatisierung, Kostenbewusstsein in technischen Entscheidungen und neue Werkzeuge für Monitoring und Sicherheit. Schulungen und die frühe Einbindung der späteren Betriebsteams gehören deshalb in den Plan. Fachbereiche brauchen verlässliche Informationen zu Wartungsfenstern, Testmitwirkung und Ansprechpartnern.

06 Artefakte und Deliverables

Die folgenden Ergebnisdokumente bilden einen sinnvollen Mindestumfang. Sie sind als lebende Artefakte angelegt und werden über die Wellen fortgeschrieben.

Planung und Entscheidung

- Zieldokument mit gewichteten Entscheidungskriterien
- Workload-Inventar mit Abhängigkeiten und Datenklassifikation
- Strategie je Workload („7 R“) mit Begründung
- Business Case inkl. Parallelbetrieb und Befähigung
- Wellenplan und Risikoregister

Plattform und Betrieb

- Zielbetriebsmodell mit Rollen und Prozessen
- Zielarchitektur und Landing Zone als Code
- Sicherheits-, Berechtigungs- und FinOps-Konzept
- Cutover-Runbooks mit Go/No-Go- und Rollback-Kriterien
- Übergabeprotokoll, Betriebshandbuch, Abschlussbericht je Welle

07 Erfolgsfaktoren und Risiken

Erfolgsfaktoren

- **Klare Entscheidungsrechte** für Strategie je Workload, Ausnahmen und Go/No-Go.
- **Ehrliches Assessment:** Inventarlücken werden als Risiko geführt.
- **Plattform vor Geschwindigkeit:** Landing Zone und Betriebsmodell vor dem Hochfahren der Wellen.
- **Wiederholbarkeit:** Runbooks und Vorlagen, die mit jeder Welle besser werden.
- **Betrieb früh einbinden**, spätestens ab der Pilotwelle.

Risiken und Gegenmaßnahmen

- **Unentdeckte Abhängigkeiten** – Discovery plus Interviews; Prüfung als Welleneingangskriterium.
- **Latenzprobleme** – gekoppelte Systeme gemeinsam migrieren, Lasttests vor dem Cutover.
- **Lizenzrisiken** – Cloud-Lizenzbedingungen vor der Strategieentscheidung prüfen.
- **Kostenüberraschungen** – Tagging-Pflicht und Budgets ab dem ersten Workload.
- **Fehlgeschlagener Cutover** – geprobte Runbooks, geprüfter Rollback.

08 Checkliste

Die Checkliste dient als Selbsttest vor dem Start und als Abnahমেhilfe je Welle.

VOR DEM START

- Ziele, Kriterien und Plattformansatz sind vom Management bestätigt.
- Workload-Inventar mit Verantwortlichen, Abhängigkeiten und Datenklassifikation liegt vor.
- Vorgaben zu Speicherort, Zugriff und Auslagerung sind erhoben.
- Zielbetriebsmodell inkl. Shared-Responsibility-Zuordnung ist beschrieben.
- Landing Zone deckt die ersten Wellen ab; Richtlinien, Logging und Tagging sind aktiv.
- Business Case enthält Parallelbetrieb, Migration, Schulung und Stilllegung.

JE WELLE UND ZUR ÜBERGABE

- Umfang, Termine, Verantwortliche und Strategie je Workload sind festgelegt.
- Abhängigkeiten sind geprüft, betroffene Partner informiert.
- Runbook, Go/No-Go-Kriterien, Point of no Return und Rollback sind geprobt.
- Budgets, Kostenberichte und Hypercare-Endkriterien sind vereinbart.
- Betriebshandbuch, Monitoring, Backup-Tests und Eskalationswege sind vom Betrieb abgenommen.
- Altumgebung ist stillgelegt; Lessons Learned sind dokumentiert.

09 Der nächste Schritt

Ein sinnvoller Einstieg ist eine kompakte Standortbestimmung: Welche Ziele verfolgt die Cloud-Transformation, wie belastbar ist das Inventar, welche regulatorischen Rahmenbedingungen gelten, und wie weit sind Betriebsmodell und Zielplattform definiert? Daraus ergeben sich die Prioritäten für Assessment, Landing Zone und Pilotwelle. Ebenso nützlich ist ein kritischer Blick auf ein bereits laufendes Vorhaben: Wo fehlen Entscheidungsgrundlagen, wo stockt die Übergabe, wo sind Kosten nicht zugeordnet? DIP unterstützt dabei mit Initialanalyse, gemeinsam mit dem Management definierten Entscheidungskriterien, einem auf Ihre Situation abgestimmten Migrationsprozess, der Koordination der ausführenden Teams und technischer Unterstützung in der Umsetzung.

10 Quellen und Standards

Im Text genannte, öffentlich verfügbare Rahmenwerke, anbieterneutral und ohne Wertung aufgeführt; ihre Nennung ist keine Zusage einer Konformität oder Zertifizierung.

- NIST Special Publication 800-145, „The NIST Definition of Cloud Computing“ (2011).
- BSI: Cloud Computing Compliance Criteria Catalogue (C5).
- FinOps Foundation: FinOps Framework.
- AWS Cloud Adoption Framework und AWS Well-Architected Framework.
- Microsoft Cloud Adoption Framework for Azure und Azure Well-Architected Framework.
- Google Cloud Adoption Framework und Google Cloud Architecture Framework.
- Verordnung (EU) 2016/679 (DSGVO), Kapitel V.
- „R“-Migrationsstrategien: Branchenkonvention, in Analysten- und Anbieterpublikationen in Varianten beschrieben.

Lassen Sie uns sprechen

Für Infos zu diesem und weiteren spannenden Themen freuen wir uns auf den Austausch mit Ihnen!

UNTERNEHMEN

DIP Deutsche IT und
Projektberatungsgesellschaft mbH
Rahmannstraße 11 · 65760 Eschborn
info@dip-consulting.de
dip-consulting.de

IHR ANSPRECHPARTNER

Manuel Fernandez

Management Consultant, Geschäftsführer
info@dip-consulting.de

Seit 2013 ist Herr Fernandez Geschäftsführer der Deutschen IT und Projektberatungsgesellschaft und seit 16 Jahren als IT-Berater in vielfältigen Rollen bei strategischen als auch bei implementierungsnahen Projekten im Einsatz.

