BMC STRATEGY CONSULTANTS

Von Cloud-Mythen zur Cloud-Strategie –
Der Weg zum Risiko-adäquaten Cloud-Zielbild in Versicherungen

Diskussionspapier

Frankfurt, im November 2020

Inhalt

Die Versicherungs-IT adaptiert immer schneller Cloud-Dienstleistungen – klare, faktenbasierte Cloud-Strategien liegen aber nicht immer vor

Pull-Effekt: Hyperscaler dringen in den Markt mit attraktiven Leistungsperspektiven

- „Attraktiver Kostenvorteil“
- „Mehr Agilität und Geschwindigkeit“
- „Stabil und Sicher“
- „Skalierte Zukunftstechnologie“
- „Risiken und Regulatorik im Griff“

Google aws Microsoft Azure

Umgang mit Cloud?

Häufig keine klare Antwort zur strategischen Fragestellung:
„Warum mit welchem System bei welchem Risiko in die Cloud bzw. warum nicht?“

- Starke Zunahme SaaS-Inseln und BMAs
- Cloud-Projekte von „Pflicht“ (MS Office 365) bis „Kür“ (Data Analytics) laufen
- Perspektivisch (“dramatische“) Reduktion Enterprise IT – bis zum „Ende des Rechenzentrums“?

Push-Effekt: On-Premise Enterprise-IT „schrumpft“ auch in Versicherungen

Cloud-Technologie ist dabei eine zentrale Voraussetzung zur Sicherstellung der langfristigen Wettbewerbsfähigkeit auch in Versicherungen

Potenzielle Nutzenvorteile der Cloud-Technologie

Geschäftsagilität

Steigerung der Geschäftsagilität durch höhere **Innovationskraft**, verbesserte **Time-to-Market** und schnellere **Skalierbarkeit**

Qualität

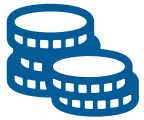
Qualitätssteigerung durch höhere **Verfügbarkeit**, geringere **Fehlerquote in der Entwicklung** und erhöhte **Testqualität**

Technologische Zukunftsfähigkeit

Sicherstellung der technologischen Zukunftsfähigkeit durch state-of-the-art **Infrastruktur-Technologie** und Ermöglichung einer modernen Micro-services Architektur

Risiko

Reduktion von Cyber Risk und Bereitstellung redundanter Infrastrukturen; Gegenläufige Effekte durch politische Risiken



Gesamtkosten/TCO

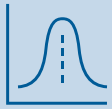
Erzielung von nachhaltiger Effizienzsteigerung durch **Reduzierung der Sach- und Personalkosten** möglich **(Potenzial)**

Innerhalb der Versicherungen führen „Cloud-Mythen“ mitunter zu gravierenden Fehleinschätzungen im Sinne einseitig positiver Bewertung oder ….

Positive Cloud-Mythen …	… BMC-Sicht und Praxisrealität
€ **„Cloud spart** uns in Run und Change **> 30% der IT-Kosten“**	▪ Für „stabile, gleichmäßige“ Nutzungsformen führt Cloud oft zur IT-Kostenerhöhung („Taxi vs. eigener PKW“) ▪ Interne Transformationsaufwände werden unterschätzt
„Unsere Business-Lines brauchen die Cloud zur **Digitalisierung“**	▪ Agilisierungsvorteile primär durch PaaS; dagegen haben IaaS und SaaS andere Zielsetzungen ▪ Interne Demand-Governance für Agilisierung wichtiger
„Enterprise IT stirbt aus; wir machen nur noch virtuelle Microservices“	▪ Aus technologischen (z.B. Mainframe) und Risiko-Gründen (Daten) wird ein Kernbestand der „On-premise“ IT bleiben
„Die Hyperscaler machen uns **compliant und sicher“**	▪ Das Risikoprofil ist bei umfassendem Cloud-Outsourcing erfordert „Risk Acceptances“ durch Vorstand ▪ Tail-Risks (Politik, Datenschutz) sind dabei relevant

Ergebnis: Oft einseitig positive Wahrnehmungen bei signifikanten Kosten- und Leistungsrisiken

… einseitig negativer Bewertung

Negative Cloud-Mythen …	… BMC-Sicht und Praxisrealität
 „Es gibt **regulatorische Show-Stopper** für die Cloud	De facto keine Show-Stopper, nur ggf. „enge“ Anforderungen an Auslagerung, Exit-Strategie, Datenschutz etc. (EBA-AL Richtlinie, DSGVO, …)
 „Cloud ist eine **technologische Modeerscheinung** – wie z.B. SOA“	Cloud bzw. Virtualisierung und Container-Ansatz ist das nächste universale IT-Paradigma – vergleichbar mit dem Schritt „Mainframe-Cobol“ auf Client-Server/Java
 „Gerade das **Datenrisiko ist so hoch,** dass Cloud ausscheidet“	Die meisten Datenrisiken lassen sich durch technische und rechtliche Vorkehrungen mitigieren
 „Risiken der Cloud sind vielfach **höher als im normalen Outsourcing“**	Rechtlich ist die Cloud-Auslagerung eine Unterform des normalen Outsourcings; es bestehen besondere, aber nicht strukturell andere Risiken und reg. Anforderungen

Ergebnis: Oft einseitige Cloud-Verweigerung bei de-facto ungesteuerter Cloud-Migration wo unvermeidbar (SaaS-Inseln, MS Office 365)

Beispiel: Positive Kosteneffekte können unter bestimmten Bedingungen und Voraussetzungen eingeholt werden

Hebel für Kosteneffekte	Positivbeispiel Cloud	Negativbeispiel Cloud
Preismodell „per use“	Nutzung Cloud für temporäre Spitzen-lasten; nicht genutzte Services werden nicht bezahlt	Dauernutzung Cloud Services bei hoher Auslastung der Infrastruktur kann Kosten erhöhen
Preisniveau pro Einheit	Attraktive Rabattstaffeln und Nutzung von Wettbewerb für Preisverhandlungen	Lock-in Risiko und Preisauftrieb
Prozessoptimierung/ Automatisierung	Proaktive interne Automatisierung Entwicklungs- und Testprozesse	Prozesse werden „as-is“ beibehalten
Migrations- und Schnittstellenkosten	Anbieter trägt Migrationskosten, klare Schnittstellen	Versicherung trägt Migrationskosten, komplexe Schnittstellen
	„Cloud günstiger“	„Cloud teurer“

Regulatorische Vorgaben stellen hohe Ansprüche an eine risikoadjustierte Gestaltung des Cloud-Outsourcing-Verhältnisses sowie Datenschutz

Regulatorische Anforderungen

EIOPA/BaFin: MaGo, MaComp & VAIT[1)]

- **MaGo**: Anforderungen an die Umsetzung von IT-Sicherheit
- **MaComp**: Umsetzung von Verhaltens-, Organisations- und Transparenzpflichten
- **VAIT**: Gibt einen Rahmen für die technisch-organisatorische Ausstattung der Institute, insbesondere für Auslagerungen und das IT-Risikomanagement

EBA Auslagerungs-richtlinie Übertrag auf Versicherungsrecht

- Richtlinien gehen über die Regelungen der **MaGo** und **VAIT** hinaus, darunter z.B.:
  - Definition von kritischen und wesentlichen Funktionen
  - Ganzheitliches Governance-Rahmenwerk
  - Anforderungen an notwendige Abklärungen und Analysen im Rahmen des Auslagerungsprozesses
  - Zudem werden Anforderungen an u.a. Sicherheit von Daten und Systemen, Beaufsichtigung der ausgelagerten Funktionen und Ausstiegsstrategien festgehalten

DSGVO

- Einrichtung von **technischen und organisatorischen Maßnahmen**, z.B.: Mandantentrennung, Löschkonzepte, Ort der Datenspeicherung, Verschlüsselung
- Berücksichtigung von **Unterauftragsverhältnissen**, Festlegung von Kontrollrechten des Cloud-Nutzers und entsprechende Duldungs- und Mitwirkungspflichten des Cloud-Anbieters

Weitere, kritische Themen

- **BSI Kriterienkatalog** mit Mindestanforderungen an sicheres Cloud Computing, 17 Bereiche, Orientierung an ISO 27001, z.B.
  - Organisation Informationssicherheit (OIS)
  - Sicherheitsrichtlinien und Arbeitsanweisungen (SP)
  - Identitäts- und Berechtigungs-Mgt. (IDM)
  - Kryptographie und Schlüsselmanagement (CRY)
  - Kommunikationssicherheit (COS)
- …

Hohe regulatorische Anforderungen, risikoadjustierte Ansätze des auslagernden Instituts gefordert

1) Mindestanforderungen an das Risiko-Management; Mindestanforderungen an die Compliance-Funktion; Bankaufsichtliche Anforderungen an die IT

Um das volle Potential der Cloud Technologie zu heben sind Veränderungen in der ganzen IT-Organisation erforderlich

Erfolgsfaktoren Cloud Transition

Training und Upskilling	▪ Upskilling eine der wesentlichen Herausforderungen bei der Cloud Transition ▪ Gap-Analyse: Abhängig vom Target Operating Model neu benötigte Skill Sets identifizieren
Cloud Center of Competence	▪ Cross-funktionale Zusammenarbeitsmodelle etablieren ▪ Fokus auf schnelle Tests und Deployments von neuen Funktionalitäten in separaten, agilen Teams
Organisatorisches Change Management	▪ Organisatorische Veränderung und Upskilling erzeugen Unsicherheit und ggf. Ablehnung bei einzelnen Mitarbeitern ▪ Effektive Kommunikation, Analyse-Methoden und enge Verzahnung mit Projekten notwendig ▪ Kritischer Faktor: Frühzeitig mit aktivem Change Management beginnen
Management Support	▪ Größeres Commitment der Organisation verstärkt positive Veränderung durch Cloud Migration ▪ Konsequente Planung und Investition verstärken die Effekte der Migration - je mehr Refactoring desto mehr Kosten-/Nutzenvorteile
Schlanke und automatisierte Prozesse	▪ Effizienzgewinne nur möglich, wenn Prozesse entsprechend angepasst werden ▪ Automatisierungsmöglichkeiten direkt nutzbar machen
Neue Mechanismen der Kostensteuerung	▪ Erfolgreiche Reduktion der IT-Kosten erfordert neue Mechanismen der Kostensteuerung ▪ Einsatz von Tools zur Rechnungskontrolle und automatisierten „rightsizing“ Vorschlägen

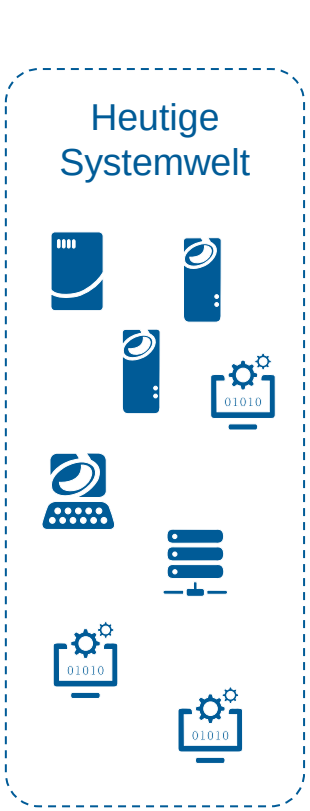
Es gibt verschiedene Ansätze zur Entwicklung einer Cloud Strategie

Fokus

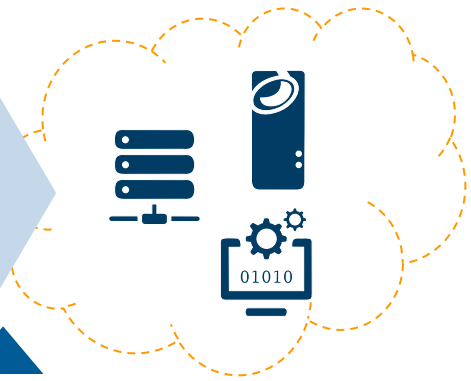
	„Summe der Einzelprojekte“	„Agil – variabel“	„Infrastruktur-orientiert“	„Rollierend-anwendungs-getrieben“	…
	▪ **Einzelne Cloud-Projekte** werden durchgeführt ▪ Cloud-Strategie entspricht der Summe der Einzel-Zielbilder	▪ Stark durch Piloten/POCs getrieben ▪ Laufende Fortschreibung der Cloud-Strategie	▪ Perspektive ist **„Rechenzentrum“ und Plattformen** (z.B. SAP HANA)	▪ Perspektive sind **fachlich-technische Anwendungscluster**	
Heraus-forderung	▪ Stimmigkeit ▪ Konsistent ▪ Nachvollziehbarkeit ▪ Leitungsfunktion ▪ Regulatorisches Risiko	▪ Stimmigkeit ▪ Konsistent ▪ Nachvollziehbarkeit ▪ Leitungsfunktion ▪ Regulatorisches Risiko	▪ Nachvollziehbarkeit und Nutzen ▪ Buy-in Fachbereich und Vorstand	▪ Einbindung Vorstand und Fachbereich ▪ Stimmigkeit aus technischer Sicht	

BMC empfiehlt ein hypothesengesteuertes Anwendungscluster-orientiertes Vorgehen zur schnellen und pragmatischen Entwicklung einer Cloud-Roadmap

In vier Schritten zur Cloud-Strategie



	1	2	3	4
	Welche Systeme in die Cloud?	Welches Cloud-Zielmodell?	Ist die Cloud vorteilhaft? Risiken?	In welchen Schritten in die Cloud?
Ergebnis-typ:	Anwendungscluster mit homogenen Eigenschaften und Anforderungen	Zuordnung Anwendungscluster zu einem Cloud Ziel-Service-/ Betriebsmodell („Vorselektion“)	▪ Je Cluster individuelle Bewertung der qualitativen und quantitativen (Business Case) Vorteile ▪ Cloud-Empfehlung je Cluster ▪ Risikobewertung	▪ Cloud-Voraussetzungen ▪ Cloud-Investitionsprogramm ▪ Cloud-Roadmap



Vorbereitende Arbeitshypothesen → Einzelbewertung → Cloud-Strategie

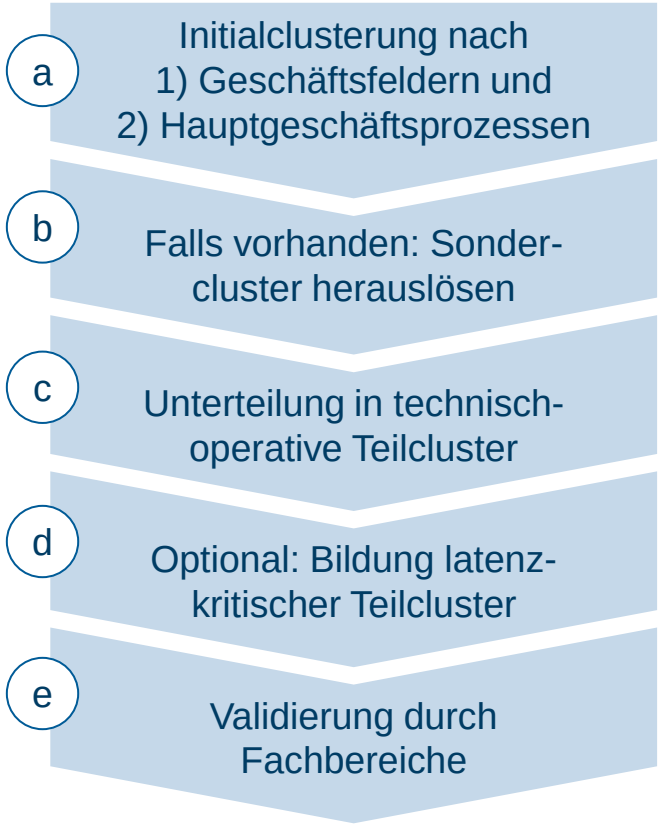
Iterationen bzgl. einzelner Anwendungen möglich

1 Welche Systeme in die Cloud? Definition von Anwendungsclustern

Ableitung potenziell Cloud-geeigneter Anwendungscluster in fünf Stufen

BMC-Erfahrungswerte:

- Bei Auswahl Cloud-geeigneter Systeme **immer von Anwendungs-systemen ausgehen** – auch wenn es „nur“ um Verlagerung der Infra-struktur geht
- Keine Einzelanwendungen be-trachten, sondern immer **Cluster** von fachlich, technisch und operativ ähnlichen (homogenen) An-wendungen
- **Fachbereiche** in abschließende Festlegung der Cluster **einbeziehen** – andernfalls Gefahr fehlender Akzeptanz



Zentrale fachliche Aspekte der Anwendungen werden im ersten Schritt berücksichtigt

z.B. Anwendungen auf Basis singulärer Techno-logie oder für spezielle Kunden werden separiert → keine weitere Betrachtung im Strategieprozess

Kriterien: Datenschutz, Schutzbedarf, Entwick-lungsmodell, Schnittstellenmenge, Volumen Datenaustausch, Batch-Jobs

Separieren latenzkritischer Anwendungen (→ aus BMC-Sicht in 3 - 5 Jahren nicht mehr erforderlich)

Notwendig zur Qualitätssicherung und Akzeptanzerhöhung

Die Rolle der IT kann sich in Richtung „Cloud Broker“ für Public Cloud verändern

Rollenwandel IT bei Hybrid Cloud Strategie

Nutzende Versicherungen

„Broker“

Vertrag & Compliance
Vertragsverhandlung/-pflege, Preismanagement, Risiko-einwertung, Datenschutz, ISM, Security etc.

Beratung
Cloud Design und Engineering, Compliance und Sicherheits-Consulting

Migrations-Projektsupport
Optimize, Legacy, Transformation, Service Design

Betrieb
Service Level, Verfügbarkeit, Automation, Cloudkompetenz

Operativer Support
Incident-, Problem- & Changemanagement, CMS, Security, Identity & Access Management

„Broker“

Microsoft Azure

Google Cloud

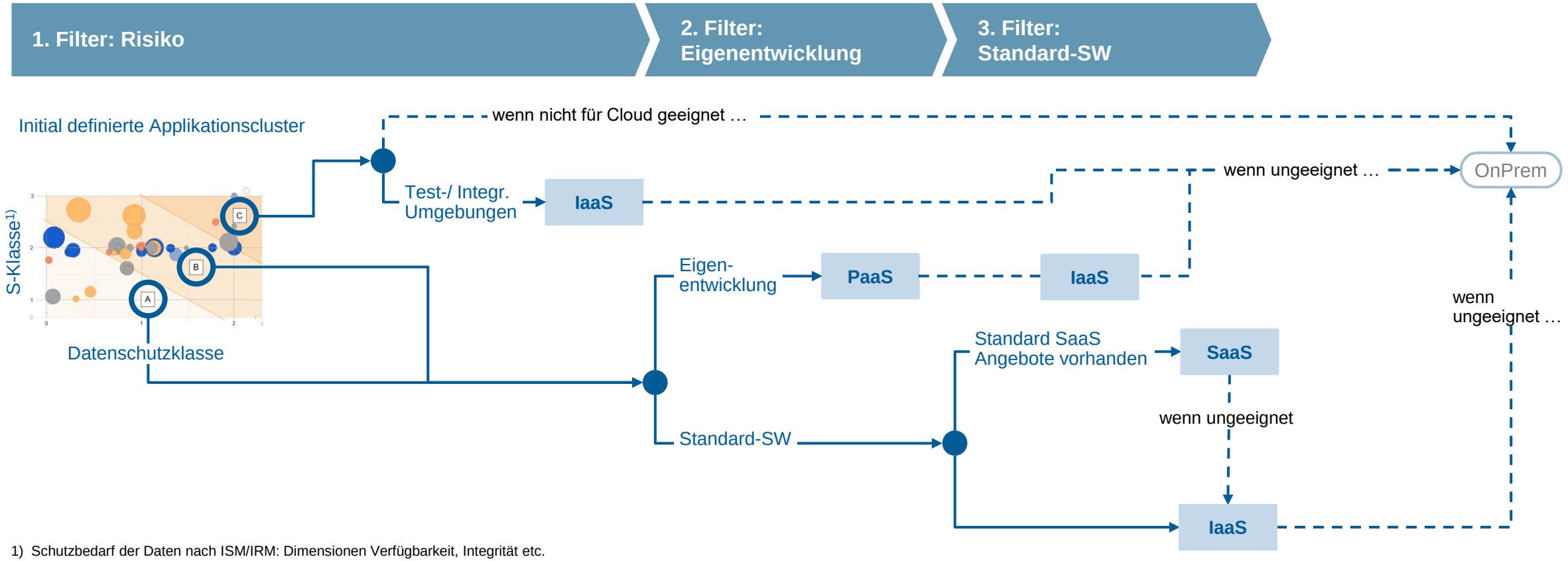
aws

Vorgehen zur Entwicklung einer Arbeitshypothese, welche (Cloud)Strategie für welches Anwendungscluster geeignet ist

Strukturierte Ableitung von Arbeitshypothesen zum zukünftigen Servicemodell über 3-stufiges Selektionsverfahren

BEISPIEL

xxx zu prüfende Arbeitshypothese

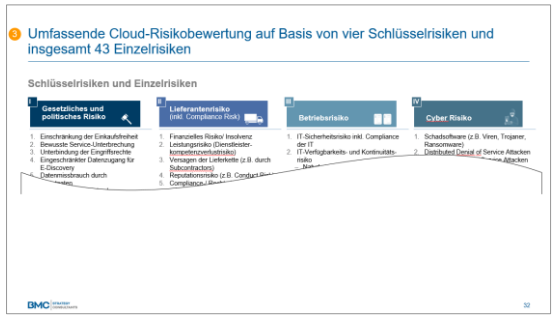


1) Schutzbedarf der Daten nach ISM/IRM: Dimensionen Verfügbarkeit, Integrität etc.

Dreistufiges, standardisiertes Vorgehen zur übergreifenden Risikobewertung

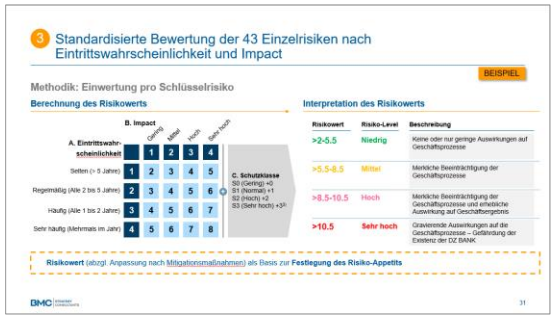
Vorgehen Risikobewertung

Schritt 1
Identifikation und Clusterung von Risiken



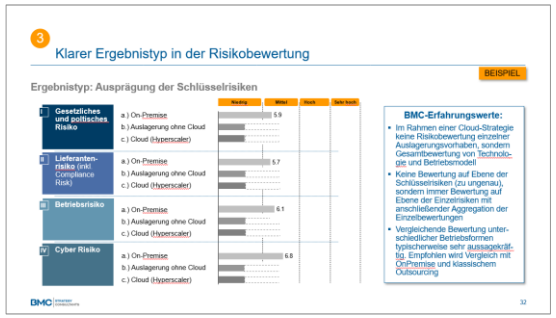
- Herleiten und Validieren von **vier Schlüsselrisiken**: Gesetzliches und politisches Risiko, Lieferantenrisiko, Betriebsrisiko und Cyber Risiko
- Sammeln von **Einzelrisiken pro Schlüsselrisiko** auf Basis interner (falls vorhanden) und externen Quellen (z.B. ENISA, Gartner)
- **Validieren** mit 2nd Line, CSOC, Auslagerungsmanagement u. ä.

Schritt 2
Bewertung der Risiken



- Einsatz einer **standardisierten Bewertungsmethodik** entlang der Kriterien „Eintrittswahrscheinlichkeit“ und „Impact“ zur Ermittlung des Risk of Exposure
- Bei Bedarf Einbeziehen der anwendungsspezifischen Schutzklassensystematik
- **Bewertung für jedes Einzelrisiko** und Aggregation zur Berechnung des Risiko-Score je Schlüsselrisiko

Schritt 3
Bestimmung Restrisiko nach Mitigation



- Identifizieren von **Mitigationsmaßnahmen** pro Einzelrisiko und Herleiten des **Restrisikos** pro Schlüsselrisiko
- Zusammenfassen der Einsichten und Aufbereiten einer Entscheidungsvorlage hinsichtlich **Risikoakzeptanz**
- **Validieren** mit 2nd Line, CSOC, Auslagerungsmanagement u. ä.

Nutzung der Public Cloud − Herausforderungen für die Finanzbranche

Microsoft Azure | Google Cloud | aws

Architektur und Technik

- EZB/BaFin/EIOPA vs. Hyperscaler Verträge
- 25 - 35 % neue oder geänderte Produkte pro Jahr
- Vertragsverhandlung mit mehreren **Arbeitsgruppen** pro Hyperscaler
- Vendor Lock-In vs. Compliance
- Zero-Trust BYOK/BYOE
- DSGVO vs. Cloud-Act
- Große Komplexität von **ca. 1.000 Produkten**

Verträge und Regulatorik

- Erheblicher und kontinuierlicher Aufwand bei Vertrags- & Providermanagement
- Über **40 Verträge** in unterschiedlichsten Versionen (Bsp. Google)
- Intransparenz des Hyperscalers
- Kontinuierliche Aufrechterhaltung der Produktcompliance

Produkte und Prozesse

- Intransparente Produktrisiken
- Pseudonymisierung/Tokenisierung

3 „Cloud-Readiness“ im Sinne einer skalierbaren, sicheren und effizienten Migrations- und Betriebsplattform muss systematisch hergestellt werden

Handlungsfelder Aufbau Cloud Plattform

	Architektur & Entwicklung	Prozesse & Prozesstools	Technische Anbindung/ Landing Zone	2nd-Line	Roadmap & Business Case	Cloud-Organisation & Kultur
SaaS PaaS IaaS	▪ Definition und Vorgaben für IaaS, PaaS ▪ Entwicklungs-umgebunden (inkl. Leistung/ Ausstattung) ▪ Technologiestacks ▪ Schnittstellen in und zw. Clouds/ on-Premise → EAI// Middleware ▪ Cloud Handbuch (Blueprint) sowie Spezifika der Hyperscaler ▪ Cloud-Security (Vorgaben, Tools, Pattern) ▪ CI/CD in der Cloud	▪ Service Build ▪ Change Mgt. ▪ IT Service Test ▪ Deployment Mgt. ▪ Avaliability Mgt. ▪ Capacity Mgt. ▪ SW License Mgt. ▪ Financial Contracts ▪ Service Level Mgt. ▪ Configuration Mgt. ▪ IT Information & Security Mgt. ▪ Incident Mgt. ▪ Problem Mgt. ▪ External Ops Mgt. (inkl. Provider Mgt. Monitoring und Housekeeping) ▪ Access Mgt. ▪ Request Fullfilment ▪ Prozess „Cloud-Stack-Definition“ ▪ Cloud On- und Off-boarding je Service	▪ Technische Anbindung Hyperscaler ▪ Netzwerkkonzept/ Konzept Breakouts ▪ Security Logs (Plattform, Service/ OS, Anwendung) ▪ Berechtigungen/ Entitlements in der Cloud ▪ SW-Distribution, Patches/ Images, Schwachstellen-scans/ -mgt.	▪ ISMS ▪ BCM ▪ ZAM ▪ IKS / OpRisk ▪ Cloud Governance ▪ Exit-Strategie ▪ Compliance/ Datenschutz ▪ Datenmgt. in der Cloud & Daten-klassifizierung	▪ Cloud-Roadmap 2021-2024 auf Clusterebene (inkl. Business Case) ▪ Bewertungskatalog Cloud-Readiness für Anwendungen ▪ Verprobung PaaS-Migration ▪ Bestandserhebung SaaS	▪ Definition IT-Rollen in der Cloud ▪ Organisatorischer Change und Kultur ▪ Kommunikation (IT und gesamtes Unternehmen) ▪ Rollenspezifischer Wissensaufbau (Projekt-Team und IT-MA)

4 Kriterien für die Auswahl von Piloten

Vendor setzt Standard („Muss-Move“)	▪ Office 365 „erweitert“, z.B. Teams, Sharepoint, … ▪ SAP HANA Roadmap
Geeigneter fachlicher/ finanzieller Case Bestandssystem-Migration	▪ Data Analytics ▪ Marktpreisrisiko → Große Datenmengen, KI, Verarbeitungsspitzen
Native neu	▪ Kunden-Frontends ▪ Anbindung Vertriebsplattformen/Ökosysteme
Geringes Risiko	▪ Testsysteme ▪ Admin-Tools

Klare Fragestellungen sind die Grundlage eines ergebnisorientierten Projektvorgehens

Aufgabenstellung aus BMC Projekterfahrung:

- Welche IT-Cluster …
- sollten warum (Nutzen)…
- wie und wann…
- auf welche Cloud-Dienstleistungs-/ Bereitstellungsmodelle?
- Welche Risiken bestehen dabei….,
- wie können diese Risiken reduziert/mitigiert werden…
- … und welche müssten vom VS akzeptiert werden?

Abgeleitete Fragestellungen Projekt „Cloud-Zielbild und -Vorgehen“

Welche **IT-Cluster der Versicherung** sind für eine potenzielle Cloud-Migration sinnvollerweise abzugrenzen/zu schneiden?

Welche **(z.B. Geschäfts-)Anforderungen und Zielkriterien** (Kosten, Geschwindigkeit, Qualität, techn. Zukunftsfähigkeit, Risiko) bestehen für eine Cloud-Migration?

Welche konkreten **Dienstleistungs-/Bereitstellungsmodelle** bieten sich als **„Cloud-Landeplattformen“** für die IT-Cluster an?

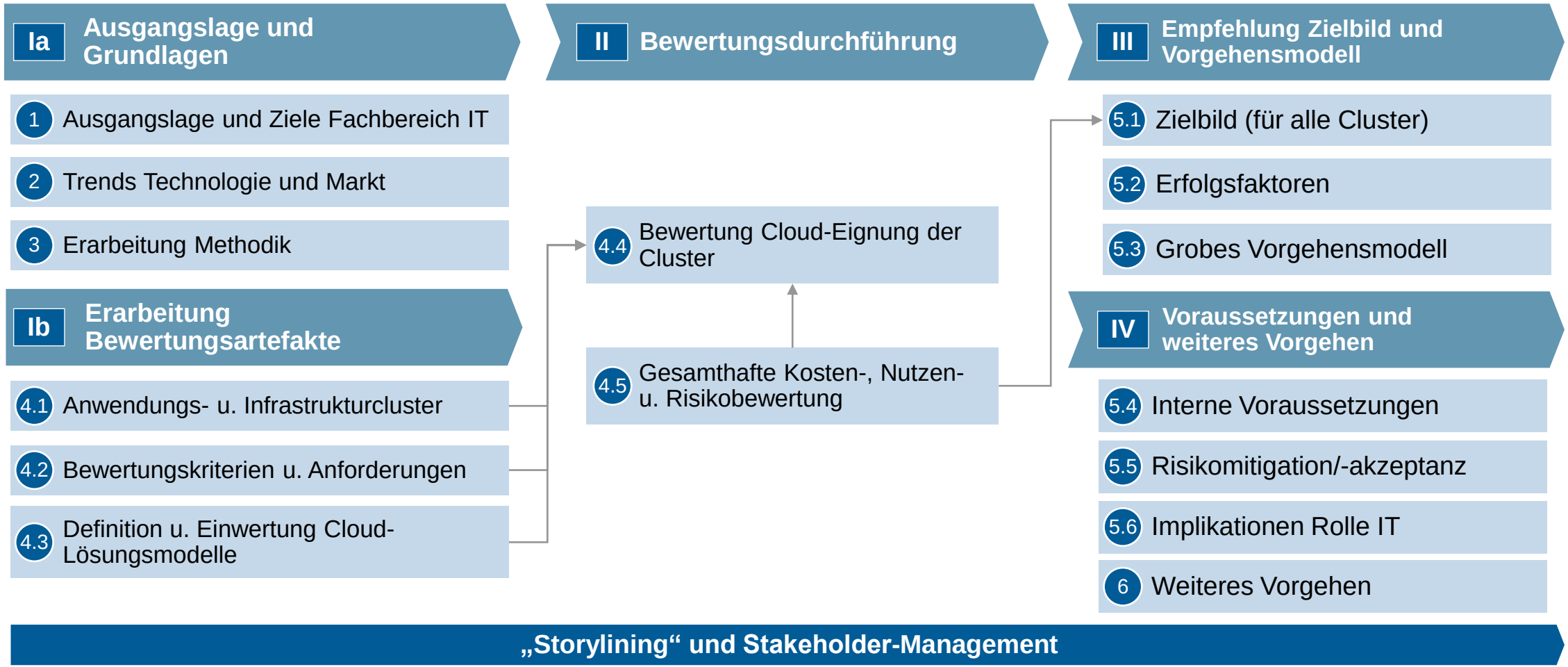
Warum (Nutzen) sollten **welche IT-Cluster** auf welche Cloud-Dienstleistungs-/ Bereitstellungsmodelle migrieren? Wann/in welcher Reihenfolge?

Welche **Risiken** bestehen? Welche Risiken können **mitigiert** werden, welche Risiken müssen **akzeptiert** werden?

Welche **internen Voraussetzungen** müssen für eine Cloud-Migration vorhanden sein?

Ein typisches Vorgehensmodell mit drei Schritten

Vorgehen für Aufgabenblock I:



BMC Strategy Consultants: Kontakt

Deutschland:
BMC Strategy Consultants GmbH

Taunus Turm, Taunustor 1
DE-60310 Frankfurt am Main
+ 49 69 50 50 60 4-586

Roland.Bubik@bmc-strategy.com
+49 170 554 1013

Thomas.Pasche@bmc-strategy.com
+49 175 290 5018

Schwesterfirma in Österreich:
BMC Professionals GmbH

Tuerkenschanzplatz 7/4
AT-1180 Wien
+ 43 6604 968608

Roland.Kropf@bmc-professionals.com