IT-Risikomanagement in Outsourcing-Beziehungen (Praxisvortrag)

CAST e.V. Workshop, 28.09.2017

Referentin: Kirsten Messer-Schmidt / excepture

Sprecherin der Fachgruppe „Management von Informationssicherheit“ der Gesellschaft für Informatik e.V.

Kirsten Messer-Schmidt

- Managing Director der Firma **excepture** in Bonn
- Senior Consultant / Business Coach mit den Schwerpunkten: Projektmanagement, Governance, Risk, Compliance, Information Security und Kommunikationsmanagement

- T.I.S.P., Senior Expertin Internal Control, ISO 27001 und IT-Grundschutz, Cyber Security Practitioner
- Lead Auditor ISO 22301
- Risk Manager (TÜV)
- PRINCE2 Practitioner, Scrum Master
- Zertifizierte Personal Coach

- Sprecherin des Leitungsgremiums der Fachgruppe Management von Informationssicherheit, GI e.V.
- Mitglied des Prüfungsausschuss für IT-Strategic / Operative Professionals der IHK Köln

Ausgangslage

Berlin, 17. Mai 2016: Die große Mehrheit der Unternehmen in Deutschland setzt bei ihrer IT auf externe Dienstleister. […] Demnach haben 82 Prozent der befragten Unternehmen Teile ihrer IT-Leistungen ausgelagert.*

* Quelle: https://www.bitkom.org/Presse/Presseinformation/Outsourcing-Fast-alle-Unternehmen-kaufen-IT-Leistungen-extern-ein.html

Motivation für IT-Outsourcing

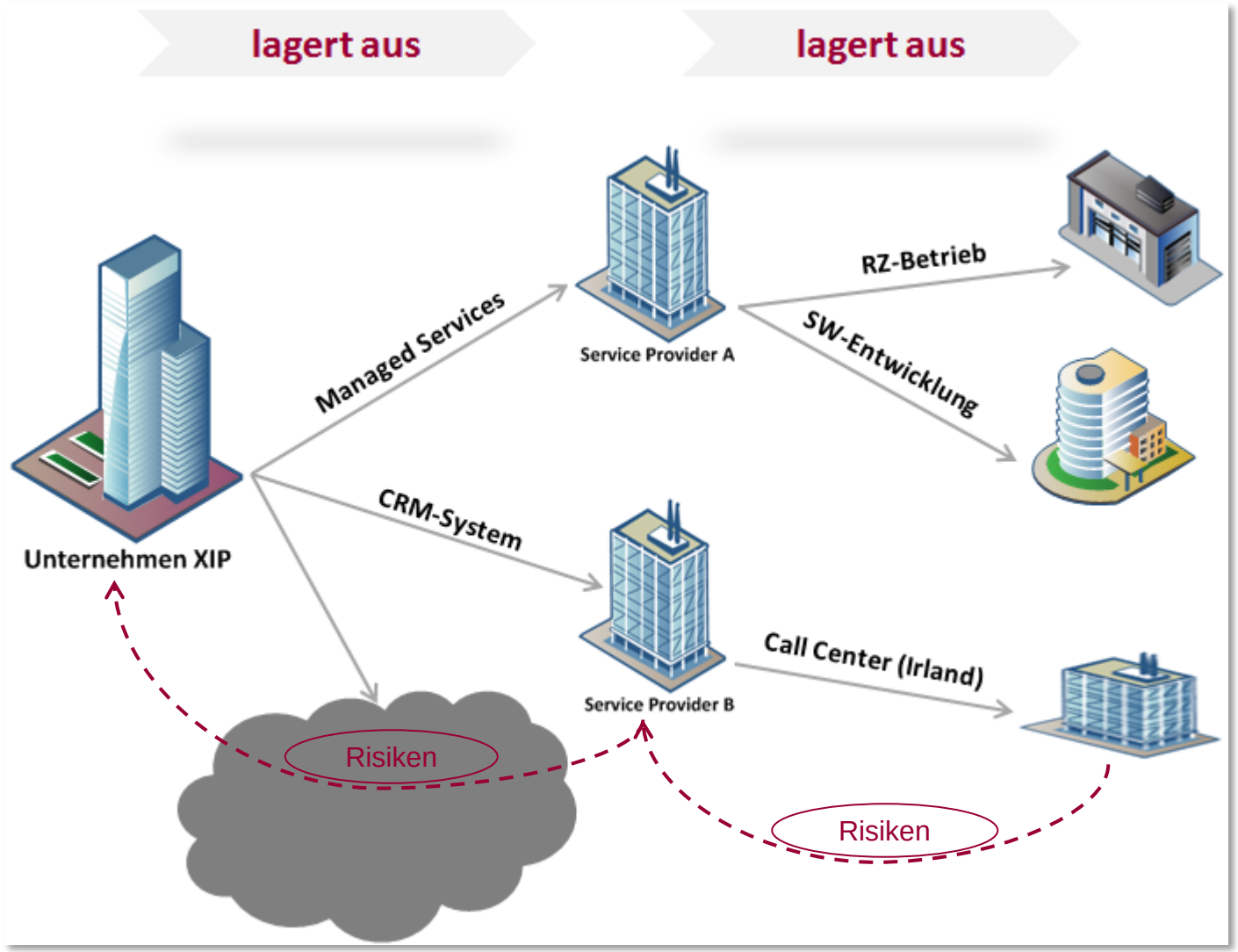
Motivation

- zunehmende Spezialisierung
- Kostendruck
- flexibler Reaktionsbedarf auf sich wandelnde Markterfordernisse
- fehlendes internes Know How oder fehlende Ressourcen

Outsourcing-Szenarien

- Business Process Outsourcing
- Outsourcing der IT-Entwicklung
- Nutzung von Cloud-Lösungen
- Managed Services
- SAS
- Hosting
- Housing
- Outsourcing IT-Betrieb oder RZ-Betrieb
- uvm.

Auslagerungsszenarien



excepture

Veränderte Risikosituation bei bleibender Verantwortung

- Die Verantwortung für Produkte und Dienstleistungen bleibt trotz Outsourcing beim auslagernden Unternehmen.
- Durchführungsmängel, Sicherheitsprobleme oder Compliance-Verstöße des Dienstleisters bleiben Risiken des Auslagerers.
- IT-Outsourcing verändert die Risikosituation des auslagernden Unternehmens → **vom IT-Risiko zum Dienstleister-Risiko**.

Risikobehandlung: Kontrollmechanismen zur Prüfung der Ordnungsmäßigkeit der externen Durchführung und der Einhaltung von Gesetzen

*In **regulierten Branchen** wie dem Bankensektor gibt es darum explizite Vorgaben zum Risikomanagement bei Outsourcing z.B. in den MaRisk.*

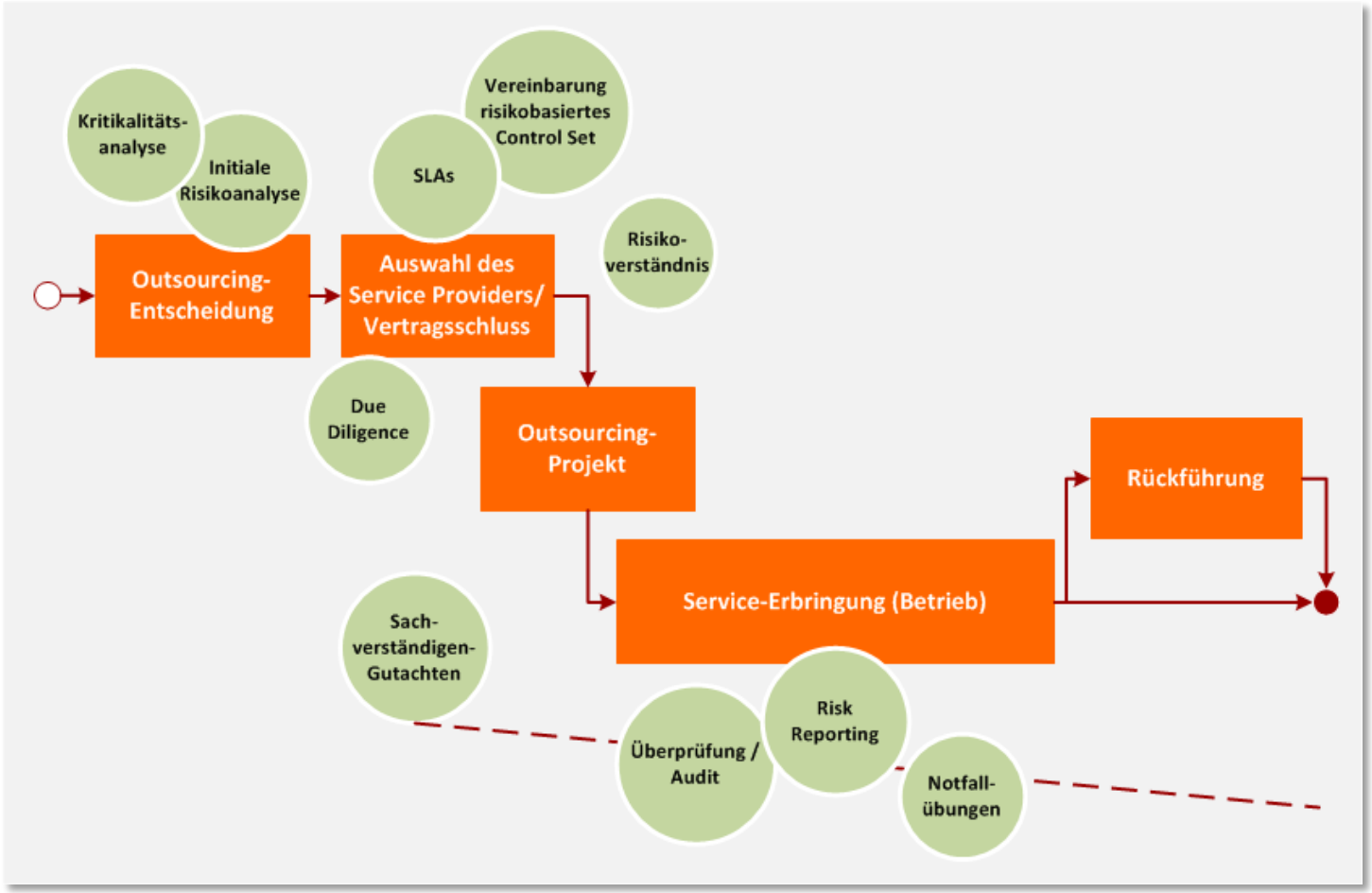
Risiken mit Auswirkung auf z.B. Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität, Qualität (beispielhaft)

Typische IT-Risiken
Infrastruktur- oder Systemausfall
korrupte Daten, Datenverlust, Ausspähen von Daten
Software-Fehler
Performance-Probleme
veraltete Hardware
fehlendes Backup
Systeme ohne Wartung, alte Patch-Stände
fehlende Kapselung, mangelnde Systemhärtung ...

Typische Outsourcing-Risiken
Kommunikations- /Verständnisprobleme, unklare Vereinbarungen
fehlende Fachkompetenz, ungeeignete Ressourcen
Terminverzug, Lieferschwierigkeiten
keine Notfallfähigkeit
Dienstleister-Ausfall
unzureichende Qualität
Verletzung gesetzlicher Vorgaben
fehlende Kontrollrechte, keine Exit-Strategie

Lifecycle des IT-Outsourcings

Management der IT-Outsourcing-Risiken über den gesamten Lifecycle und über alle Ebenen der Auslagerung



excepture

Vor der Auslagerung

Basis für die Auswahl geeigneter Outsourcing-Varianten und eines passenden Service Providers

- Festlegung des Outsourcing-Ziels und -Scopes
- Einschätzung der Kritikalität des ausgelagerten Prozesses, des Systems oder der Funktion und grobe Risikoanalyse
- Ermittlung der rechtlichen Rahmenbedingungen

Kritikalitätsanalyse

Grundlage für die Einschätzung von IT-Outsourcing-Risiken: **Feststellung der Kritikalität** der Auslagerung für das eigene Unternehmen (u.a. abhängig von der eigenen Branche)

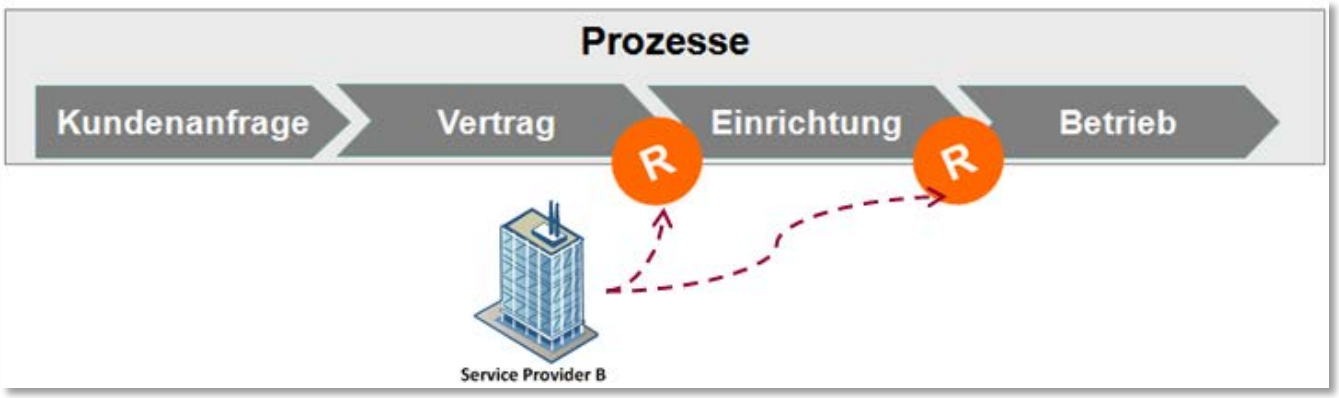
Kriterium	Bewertung	Ableitung
(Teil-)Auslagerung eines wertschöpfenden Prozesses	j/n	
Häufigkeit des Bezugs der externen Dienstleistung	x-mal	
Komplexität der Dienstleistung (Know How, Technik, Schnittstellen, Subunternehmerebenen, etc.)	g/m/h	
Schutzniveau der Daten (Maximalprinzip)	j/n	
Auftragsdatenverarbeitung	j/n	
Zugriff auf verarbeitetete Daten durch DL	j/n	
besondere gesetzliche / regulatorische Rahmenbedingungen	j/n	
Anzahl der von Ausfall / Störung betroffener Kunden / Produkte und deren Priorität	x	
DL-Ausfall / Störung kompensierbar, wenn ja Art der Kompensation	j/n	
Konsequenzen bei Ausfall/Störung der Dienstleistung	j/n	
Rückabwicklung erforderlich? möglich?	j/n	

Anforderungen und Risiken

excepture

Grobe Risikoanalyse

Betrachtung der Prozess- und/oder Service-Relevanz des IT-Outsourcings zur Grobeinschätzung des Risikopotenzials



- Ermittlung möglicher Auslöser für z. B.

  Nicht-Verfügbarkeit der Dienstleistung – Verlust von Daten – Störung der Integrität von Daten – Ausspähen / Missbrauch von Daten
- Bewertung von Eintrittswahrscheinlichkeit und Schadensausmaß

Outsourcing-Risiken beim auslagernden Unternehmen

- fehlende Outsourcing-Strategie
- Beauftragung unterschiedlicher Dienstleister
- unzureichende Dienstleistersteuerung
- fehlende Vorgaben z. B. Sicherheitsanforderungen, Entwicklungsvorgaben
- fehlendes Personal / Know How
- nicht kalkulierter Aufwand für die Anpassung interner Prozessen
- interner Administrationsaufwand
- Migrationsaufwand, -kosten

Service-typische Risiken

Risiken beim Dienstleister

Service-typische Risiken

Cloud Computing – Benefits, risks and recommendations for information security

Policy and organizational risks

- R.1 Lock-in
- R.2 Loss of governance
- R.3 Compliance challenges
- R.4 Loss of business reputation due to co-t
- R.5 Cloud service termination or failure
- R.6 Cloud provider acquisition
- R.7 Supply chain failure

Technical risks

- R.8 Resource exhaustion (under or over pr
- R.9 Isolation failure
- R.10 Cloud provider malicious insider - abus
- R.11 Management interface compromise (n
- R.12 Intercepting data in transit
- R.13 Data leakage on up/download, intra-cl
- R.14 Insecure or ineffective deletion of data
- R.15 Distributed denial of service (DDoS)
- R.16 Economic denial of service (EDOS)
- R.17 Loss of encryption keys
- R.18 Undertaking malicious probes or scans
- R.19 Compromise service engine
- R.20 Conflicts between customer hardening

Legal risks

- R.21 Subpoena and e-discovery
- R.22 Risk from changes of jurisdiction
- R.23 Data protection risks
- R.24 Licensing risks

R.10 Cloud provider malicious insider - abuse of high privilege roles

Probability	MEDIUM (Lower than traditional)	Comparative: Lower
Impact	VERY HIGH (Higher than traditional)	Comparative: Higher (aggregate) Comparative: Same (for a single customer)
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V36. Need-to-know principle not applied V1. AAA vulnerabilities V39. System or OS vulnerabilities V37. Inadequate physical security procedures V10. Impossibility of processing data in encrypted form V48. Application vulnerabilities or poor patch management	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

November 2009

excepture

Dienstleisterauswahl (Cloud)

Informationen zur Beurteilung der Risiken auf Seiten eines Service-Anbieters (z. B. Cloud Service)

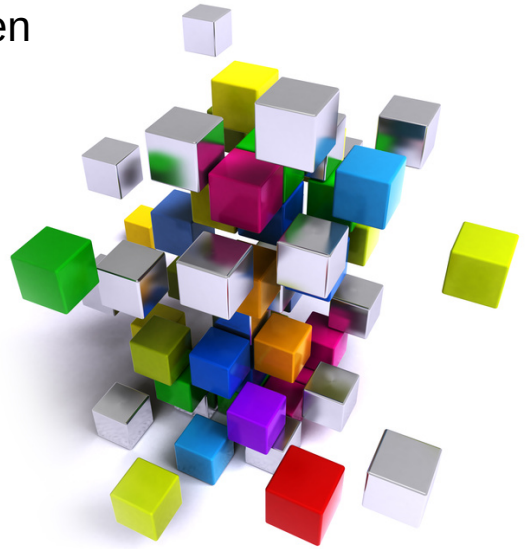
Vertragsschluss (1 /2)

Vereinbarung der Instrumente, die zur Risikosteuerung benötigt werden, in Abhängigkeit von der Art der Auslagerung und der eigenen Branche

Vertragsschluss (2/2)

Instrumente zur Steuerung von IT-relevanten Dienstleisterrisiken, die je nach Kritikalität des Outsourcings vereinbart werden sollten:

- Einräumung von Prüf- und Kontrollrechte
- Prüf-Nachweise von sachverständigen Dritten: Zertifikate / WP-Bescheinigung wie etwa IDW PS 951
- Vereinbarung eines kundenspezifischen risikobasierten Control Sets (*Orientierung an COBIT, IT-Grundschutz oder anderen Leitlinien)*
- **Vereinbarung von Risikomanagement- und Berichtsstrukturen**
- Vereinbarung (gemeinsamer) Notfallübungen
- Vereinbarungen zum Umgang mit weiteren Subunternehmer-Ebenen
- …



UP KRITIS

Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen

Empfohlene Anforderungen an jeden Auftragnehmer:

Vulnerability-Management, Patch-Management, Systemhärtung, Fernzugang für Drittanbieter, Anforderungen an die Softwareentwicklungsprozesse für Einsatz der kryptographischen Lösungen, Dokumentation, Benachrichtigung über sicherheitsrelevante Vorfälle, Nicht-technische Sicherheit

Empfohlene Anforderungen an Auftragnehmer, die neben Softwarelösungen weitere Dienstleistungen erbringen z.B. IT-Betrieb, Remote-Support:

Informationssicherheitsprozesse / ISMS, Zugriffsschutz / Berechtigungsvergabe, Asset-Management, Personalsicherheit, physische Sicherheit / Zutrittsschutz, operationelle IS-Anforderungen […] Sicherheit in der Softwareentwicklung, Change-Prozesse, Security-Incident-Management, Sicherheit in Auslagerungsprozessen

vom 05.07.2016

Risiken im Betrieb steuern

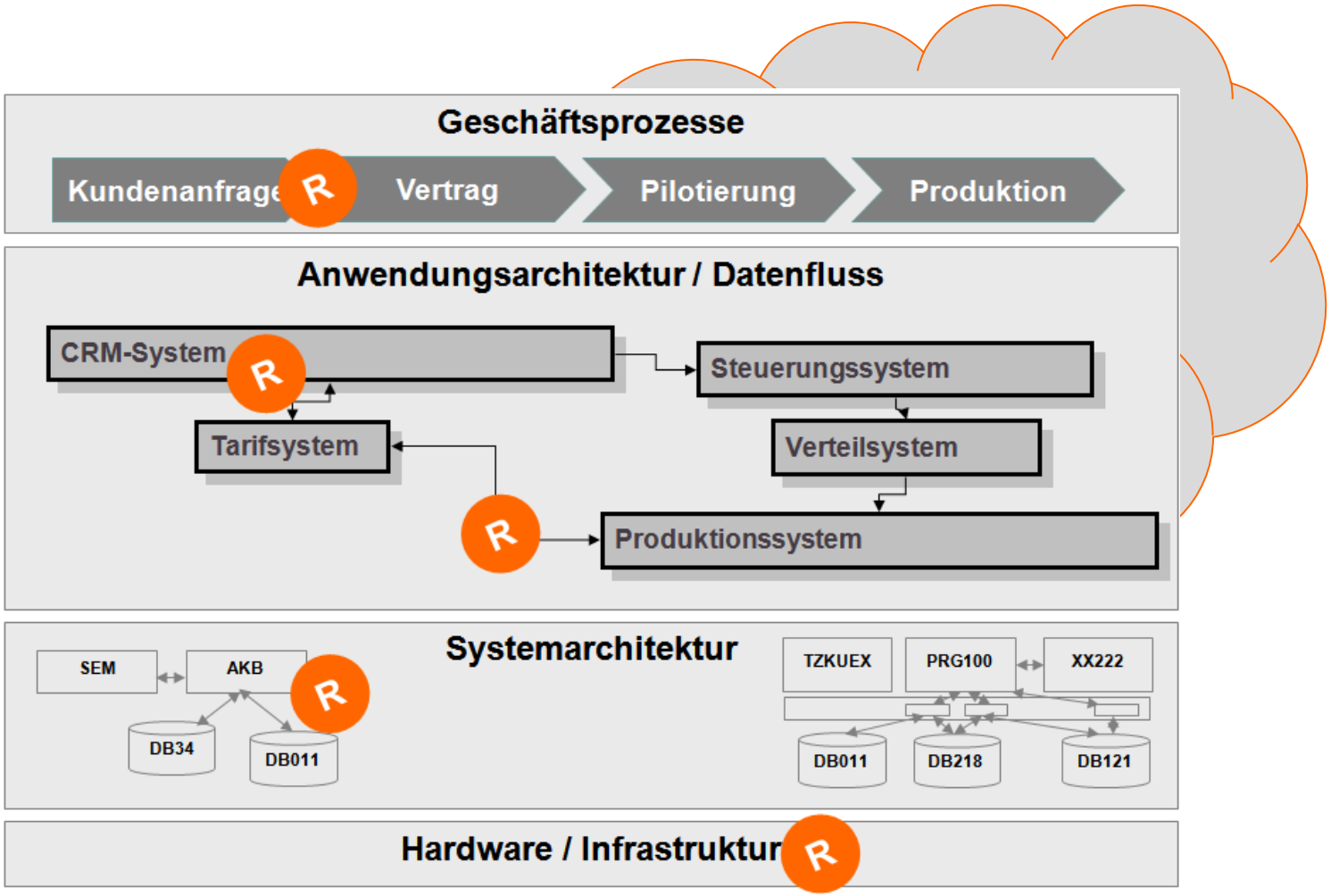
Risikoverständnis

Gemeinsame Flughöhe festlegen:

- dienstleistungsrelevante Risiko-Szenarien und ggf. Key Risk Indicator vereinbaren
- gemeinsames Verständnis erzielen über die Kriterien der Risikobewertung und die Verdichtung von Risiken
- Perspektiven abgleichen und synchronisieren
- Bewertungsrhythmus und Berichtsstrukturen festlegen

Control-basierte Risikoanalyse

Mit Blick auf die ordnungsgemäße Dientleistungserbringung



excepture

Prüfung des risikobasierten Control Sets

- durch den Auslagerer
- durch Zertifizierer und Wirtschaftsprüfer
- durch den Dienstleister selbst

Berichterstattung des Dienstleisters über

- durchgeführte interne / externe Prüfungen und ihre Ergebnisse (u.a. Penetrationstests)
- Abweichungen vom Regelbetrieb (z. B. Incidents, Notfälle)
- Schwachstellen und Risiken
- Notfallübungen und ihr Ergebnis
- SLA-Verletzungen
- etc.

Risiken bei Rückabwicklung

Fehlende Ressourcen, fehlendes Know-How im eigenen Unternehmen, keine Ausweichmöglichkeiten, keine zuverlässige Rückführung / Löschung von Daten u.v.m

Danke!

excepture®
Kirsten Messer-Schmidt

Franzstr. 9 | D-53111 Bonn
Phone: + 49 228 18031040 | Mail: o.ffice@excepture.de

Bildrechte

Folie 3	© excepture
Folie 9	© fotolia, alphaspirit
Folie 14,22	© gratisography, Ryan McG
Folie 15	© unsplash, Joao Silas
Folie 16	© fotolia, Franck Boston
Folie 18	© picjumbo, Viktor Hanacek
Folie 19,22	© stockata, CCO Public Domain

excepture