

# IT-Audit ZF

Von Mike und Luca

# Inhalt

1	Wertbeitrag IT .....	7
1.1	IT-Probleme .....	7
1.2	Wertbeitrag der IT .....	7
1.3	IT-Kostenmanagement (Overhead / CTB / RTB).....	7
1.4	IT Value.....	7
1.5	Geschäftsprozess-Automatisierung .....	8
1.5.1	Merkmale .....	8
1.5.2	Einsparungen.....	8
1.6	Risikoportfolio .....	9
1.6.1	Umstrukturierung.....	9
1.6.2	Strategischer Modus.....	9
1.6.3	Fabrikmodus.....	9
1.6.4	Supportmodus.....	9
2	Digitalisierung.....	10
2.1	Begriff .....	10
2.2	Digitale Transformation.....	10
2.3	Ansatzpunkte.....	10
2.4	Veränderungen in der Geschäftswelt.....	11
2.5	Drei Dimensionen .....	11
2.5.1	Veränderung des Geschäftsmodells.....	12
2.5.2	Organisatorische Veränderung.....	12
2.5.3	Bedeutung der Technologien für Unternehmen .....	12
2.6	Aufgabenbereiche eines CDO.....	13
2.7	Vorgehen bei der Transformation .....	13
2.7.1	6 Steps zum digitalen Wandel .....	14
2.8	Schlüsselkennzahlen.....	14
2.9	Fazit .....	15
2.9.1	Kritik und Ausblick .....	15
2.9.2	Handlungsempfehlung .....	15
2.9.3	Zusammenfassung.....	16
3	Wirtschaftlichkeitsanalyse.....	17
3.1	Kosten und Nutzen bestimmten den Wertbeitrag der IT .....	17
3.2	Business Case.....	17
3.2.1	Definition .....	17
3.2.2	Stakeholder.....	17

3.2.3	Bausteine .....	18
3.2.4	Investitionsentscheidung .....	18
3.3	Business-Case-Erstellung.....	19
3.3.1	3 Phasen .....	19
3.3.2	Vorgehensmodell .....	19
3.3.3	Nutzenfestlegen .....	20
3.3.4	Dokumentation.....	20
3.4	Social Media Business Case → Kunden Community .....	21
3.4.1	Return of Investment .....	21
3.4.2	Nutzen .....	21
3.4.3	Nutzenkategorien.....	22
3.4.4	Erstlösungsquote .....	22
3.4.5	Weitere Nutzenkategorien.....	22
3.5	Online Kunden-Community Allgemein.....	23
3.5.1	Kostenkategorien einer Online Kunden-Community .....	23
3.5.2	Initialkosten .....	23
3.5.3	Wiederkehrende Kosten.....	24
3.6	Kennzahlen .....	24
3.6.1	Diskontierung .....	25
3.6.2	Berechnungsbeispiele .....	25
3.6.3	ROI .....	26
3.7	Fazit .....	26
4	Outsourcing .....	27
4.1	Begriffsdefinition .....	27
4.2	Markt.....	27
4.2.1	Veränderungen im Service Einkauf .....	27
4.2.2	Cloud Brokering.....	27
4.3	Strategie Modell .....	28
4.3.1	Phasen Modell.....	28
4.3.2	Vom CMO zum FMO .....	29
4.3.3	Typische Fragestellungen .....	29
4.3.4	Outsourcing Scope.....	30
4.3.5	Sourcing Scope .....	30
4.3.6	Bewertung .....	31
4.3.7	Bewertung nach Baselstadt.....	31
4.3.8	Sourcing Scope, -Modell, -Szenarien.....	32

4.3.9	Sourcing Prinzipien .....	32
4.4	Argument-Bilanz.....	33
4.4.1	Strategie .....	33
4.4.2	Leistung .....	33
4.4.3	Kosten.....	33
4.4.4	Personal.....	33
4.4.5	Finanzen .....	34
4.5	Business-Case .....	34
4.5.1	Kostensenkung .....	34
4.5.2	Lösungsbewertung .....	34
4.5.3	Nutzen im Outsourcing.....	35
4.5.4	Praxisbeispiel.....	35
4.6	Erfolgsfaktoren vom Sourcing .....	36
4.7	Outsourcing-Prozess.....	36
4.8	SLA .....	36
4.8.1	Beispiel SLA.....	37
4.9	Chancen und Risiken IT-Outsourcing.....	37
5	Lizenzmanagement.....	38
5.1	Definitionen.....	38
5.2	4 Stufen der Einführung .....	38
5.3	Typische Unternehmenssituationen .....	39
5.4	Fragen für die erste Bestandsaufnahme .....	39
5.5	Weitere Verteilung der Implementierung eines Lizenzmanagements .....	40
5.6	Lizenzmodell.....	40
5.7	Haupt- und Teilprozesse im Software-Life-Cycle-Prozess .....	41
5.8	Der Lizenzmanager .....	41
5.9	Fragen zur Erfassung der Lizenz- und Nutzungsdaten .....	41
5.10	Zusammenfassung.....	42
6	Musterlösungen von Guido Kaufmann .....	43
7	IT Audit-Planung .....	49
7.1	Rahmenbedingungen .....	49
7.1.1	Ziele Prüfung Finanzberichterstattung .....	50
7.2	Timeline .....	50
8	Prüfungsdurchführung .....	51
8.1	Kontrollarten .....	51
8.1.1	Entity Level Controls.....	51

8.1.2	Process Level Controls .....	52
8.1.3	General IT Controls.....	54
8.1.4	Assertions .....	55
8.1.5	Kontrolleigenschaften .....	56
8.2	Manuelle Kontrollen.....	56
8.2.1	Stichprobenprüfung .....	57
8.3	Automatische Kontrollen.....	58
8.3.1	Prüfung .....	58
8.3.2	Benchmarking.....	59
8.4	Verhalten bei Exceptions.....	59
8.4.1	Re-testing: .....	60
8.4.2	Kompensierende Kontrollen.....	60
8.5	Attestation Reports .....	61
8.6	End User Computing.....	62
8.6.1	GITC-Kontrollen .....	62
9	IT Audit Frameworks .....	63
9.1	ISACA .....	63
9.2	Cobit .....	63
9.3	COSO.....	64
9.3.1	Dimensionen.....	65
9.4	ITIL .....	66
10	IT-Audit Dokumentation.....	67
11	Bewertung Ergebnisse.....	67
11.1	Ineffektive Applikationskontrollen.....	67
11.2	Ineffektive GITC .....	69
12	Herleitung Massnahmen .....	70
13	Vorgehensmodell Anwendungsprüfung.....	71
13.1	Grundidee.....	71
13.2	8 Schritte .....	72
13.2.1	1. Analyse .....	73
13.2.2	Geschäftsprozesse & Datenflüsse .....	73
13.2.3	Kernanwendungen und der IT-relevanten Schnittstellen .....	73
13.2.4	Risiken und Schlüsselkontrollen .....	73
13.2.5	Walk-Through.....	74
13.2.6	Beurteilung des Kontrolldesigns.....	74
13.2.7	Beurteilung der Umsetzung der Kontrollen .....	75

13.2.8	Gesamtbeachtung und Ergebnisfindung .....	75
14	Notizen zu Prüfungsfragen Controlls etc.....	75

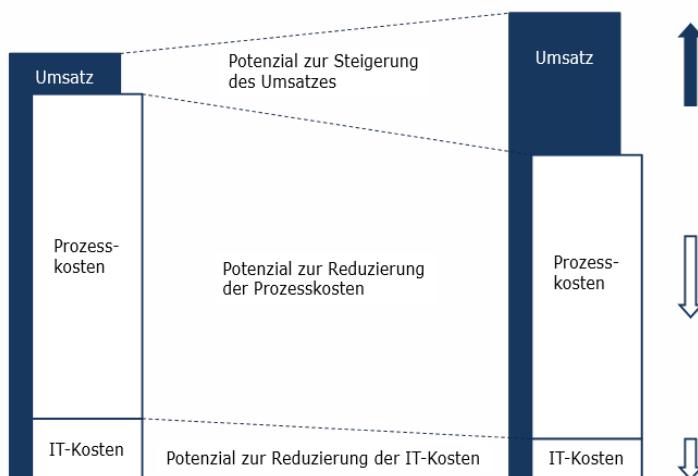
# 1 Wertbeitrag IT

## 1.1 IT-Probleme

- Produktivitätsparadoxon: Man gibt mehr für IT aus, als man zurück erhält --> Produktivität bleibt weg
- Kein direkter Gewinn
- IT kostet viel
- Nutzen ist nur schwierig messbar
- Es führt keinen Weg um die IT herum
- Man merkt erst, was man hat, wenn die IT nicht mehr funktioniert.
- IT nur als Kostenstelle
- Kommunikationsproblem zwischen Nutzer und IT

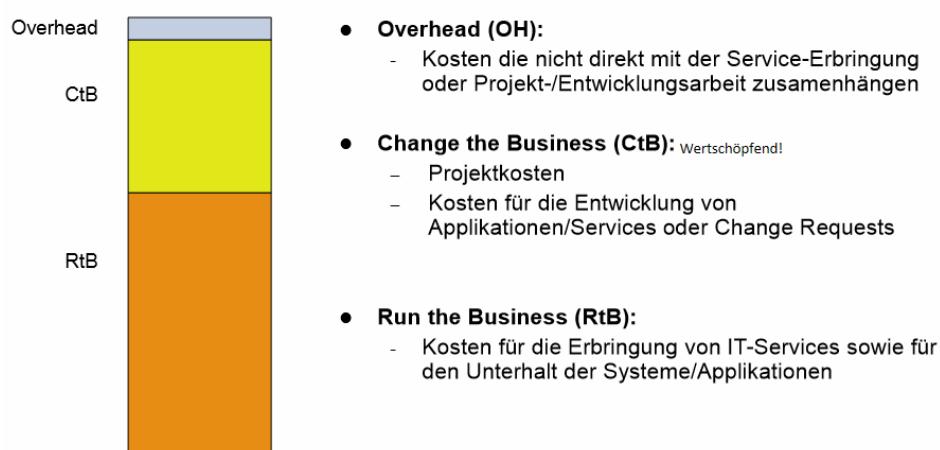
## 1.2 Wertbeitrag der IT

### Wertbeitrag: Einfluss der IT auf Umsatz und Kosten



## 1.3 IT-Kostenmanagement (Overhead / CtB / RtB)

### Elemente des IT-Kostenmanagements



## 1.4 IT Value

IT-Value = IT-Nutzen - IT-Kosten

## 1.5 Geschäftsprozess-Automatisierung

### 1.5.1 Merkmale

#### **Unternehmensübergreifende Geschäftsprozesse sind gekennzeichnet durch:**

- enge Verzahnung betrieblicher Leistungsprozesse und Kunden-/Lieferanteninteraktion
- verstärkte elektronische Steuerung der Abläufe unter steigender Einbeziehung interner u. externer Informationen
- steigende Anzahl beteiligter Partner
- Infragestellung traditioneller Abläufe

### 1.5.2 Einsparungen

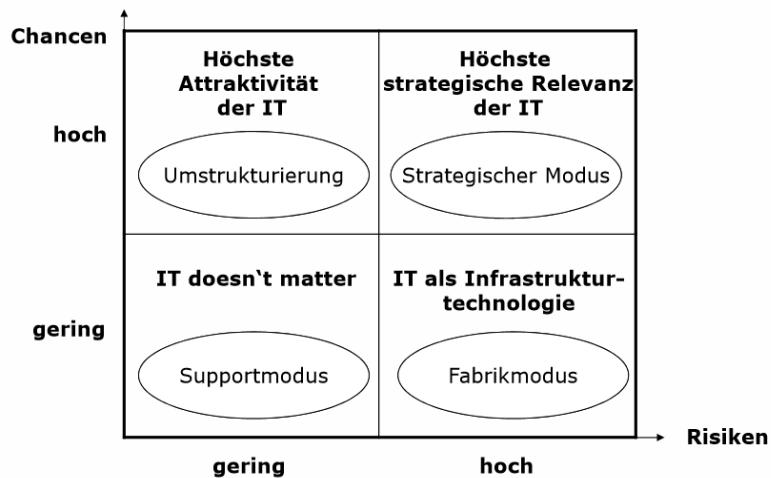
#### **Ermittlung der Prozesskosten pro Jahr**

Prozesskosten	
Personalkosten	34.7
Sachkosten	9.2
<b>Total</b>	<b>43.9</b>
Anzahl Buchungen pro Jahr	20'000
<b>Prozesskosten pro Jahr</b>	<b>877'333</b>
Personalkosten (pro Stunde)	40

Lohnt sich Investition? Wieviel kann gespart werden.

## 1.6 Risikoportfolio

Portfolioanalyse: Chancen-/Risiko-Portfolio



### 1.6.1 Umstrukturierung

- Als wesentliche Aufgaben des IT-Managements von Unternehmen im Umstrukturierungsmodus sind zu nennen:
  - Sicherstellung des finanziellen Budgets zur Nutzung der Innovationspotenziale der IT
  - Aufstockung des IT-Personals zur Nutzung der Chance
  - Veränderung der organisatorischen Einordnung der IT in die Unternehmensorganisation

### 1.6.2 Strategischer Modus

Als Kernaufgaben des IT-Managements für Unternehmen im strategischen Modus sind zu nennen:

- Permanente Abstimmung der IT-Strategie mit der Unternehmensstrategie
- Analyse der Innovationsfähigkeit der IT-Systeme
- Herstellung von Transparenz über die IT-Performance der Wettbewerber

### 1.6.3 Fabrikmodus

Die Kernaufgaben des IT-Managements für Unternehmen im Fabrikmodus liegen im Risikomanagement:

- Gewährleistung der Ausfallsicherheit durch redundante IT-Systeme und Datenhaltung
- Gewährleistung der Datensicherheit durch Vermeidung von Angriffen von aussen.

### 1.6.4 Supportmodus

Für das IT-Management ergeben sich in dieser Kategorie die folgenden Aufgabenbereiche:

- Analyse der Veränderung der strategischen Relevanz der IT (Veränderung der Chancen oder Risiken im Zeitablauf)
- Monitoring der IT-Aktivitäten der Wettbewerber
- Kosteneffiziente Steuerung der IT-Budgets (Vermeidung von unnötigen Innovationen)

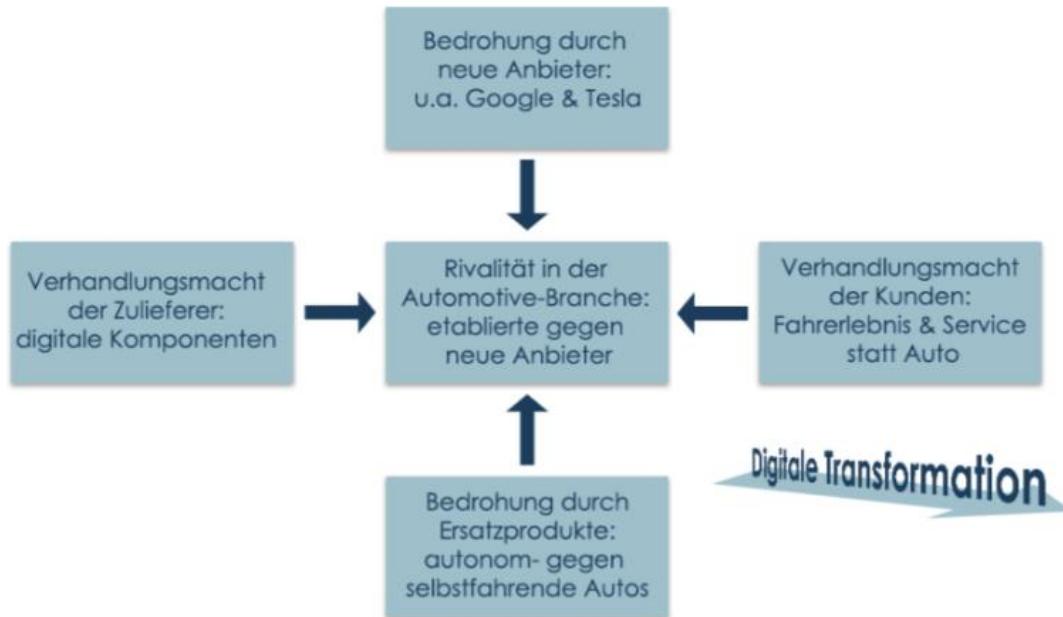
## 2 Digitalisierung

### 2.1 Begriff

Der Begriff der **Digitalisierung** hat mehrere Bedeutungen. Er kann die **digitale Umwandlung und Darstellung** bzw. Durchführung von Information und Kommunikation oder die **digitale Modifikation** von Instrumenten, Geräten und Fahrzeugen ebenso meinen wie die **digitale Revolution**, die auch als dritte Revolution bekannt ist, bzw. die digitale Wende. Im letzteren Kontext, [...], werden nicht zuletzt "Informationszeitalter" und "**Computerisierung**" genannt. Während im 20. Jahrhundert die Informationstechnologie (IT) vor allem der **Automatisierung und Optimierung** diente, Privathaushalt und Arbeitsplatz modernisiert, Computernetze geschaffen und Softwareprodukte wie Office-Programme und Enterprise-Resource-Planning-Systeme eingeführt wurden, stehen seit Anfang des 21. Jahrhunderts **disruptive Technologien und innovative Geschäftsmodelle sowie Autonomisierung, Flexibilisierung und Individualisierung** in der Digitalisierung im Vordergrund. Diese hat eine neue Richtung genommen und mündet in die vierte industrielle Revolution, die wiederum mit dem Begriff der **Industrie 4.0** (auch "Enterprise 4.0") verbunden wird.

### 2.2 Digitale Transformation

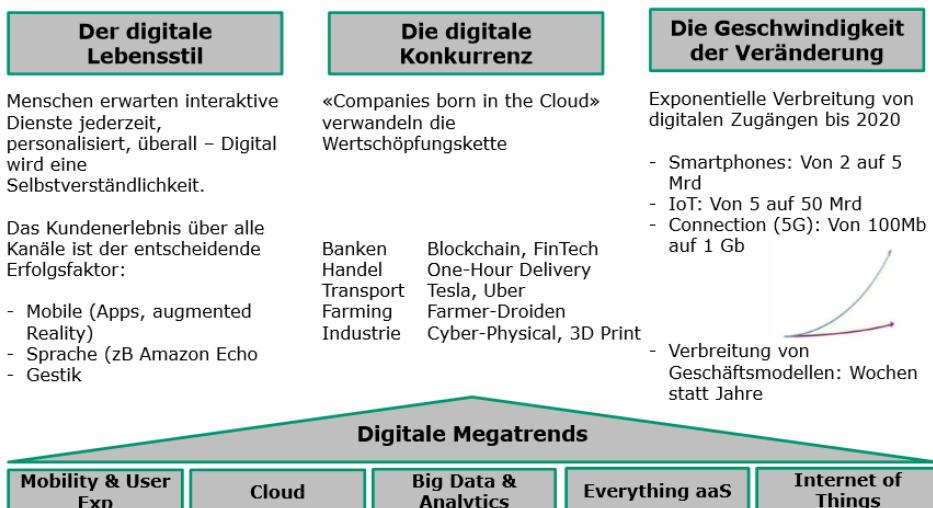
#### 5-Kräfte-Modell und digitale Transformation am Beispiel Automotive



### 2.3 Ansatzpunkte

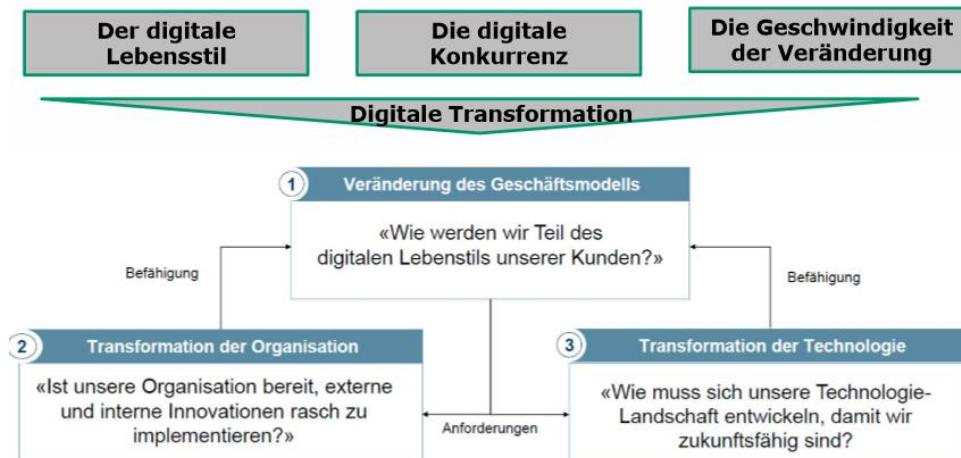
Prozesse – Produkte – Services führen zu neuen Geschäftsmodellen

## 2.4 Veränderungen in der Geschäftswelt

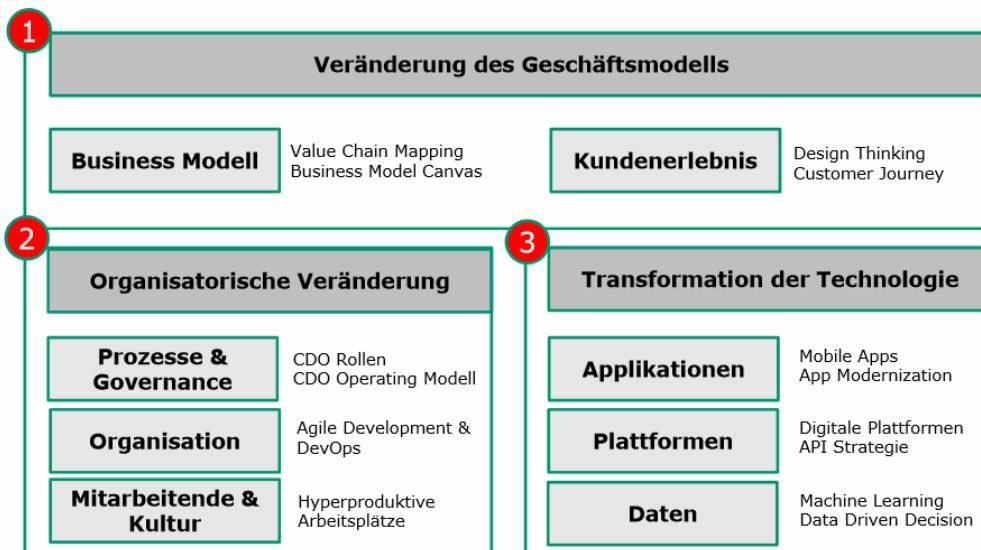


## 2.5 Drei Dimensionen

### Die Digitalisierung erfordert eine Transformation in drei Dimensionen



### Digitale Transformation der drei Dimensionen: Methoden, Modelle und Denkanstösse



### 2.5.1 Veränderung des Geschäftsmodells

Bild Customer Journey... ist alles was in den Folien steht

### 2.5.2 Organisatorische Veränderung

#### 2. Organisatorische Veränderung

##### Neujustierung mit Chief Digital Officer und Innovations-Teams

- Ein guter Ausgangspunkt für die Neujustierung ist die Etablierung eines **Chief Digital Officers**.
- Er/Sie koordiniert unternehmensweit den (digitalen) Innovationsprozess.
- Er/Sie braucht ein Team aus Sponsoren und Innovatoren mit der Bereitschaft, alles in Frage zu stellen.
- Solche Innovations-Teams, "**Digital Advisory Boards**" oder "**Digitalen Beiräte**" müssen in der Lage sein, Start-ups oder Start-up-ähnliche Strukturen ins Leben zu rufen und auf Geschäftsleitung- und VR-Ebene Ergebnisse und Vorschläge zu adressieren.



### 2.5.3 Bedeutung der Technologien für Unternehmen

Maschinenintelligenz ist Treiber der wahren digitalen Revolution.



## 2.6 Aufgabenbereiche eines CDO

- Entwicklung und Umsetzung einer **Digitalstrategie**,
- Unterstützung der Fachbereiche bei der Entwicklung und Optimierung von **digitalen Lösungen** für deren **Geschäftsprozesse**,
- Identifikation und Einführung so genannter „**Best Practices**“ für das Unternehmen,
- Förderung des **Informationsflusses** zwischen allen Gruppen des Unternehmens, die an digitalen Lösungen arbeiten bzw. mit diesen arbeiten,
- Planung, Überwachung und Analyse der **digitalen Budgets**.

## 2.7 Vorgehen bei der Transformation

### **Digitale Transformation: Wo stehen Sie? Wo wollen Sie hin?**



## 2.7.1 6 Steps zum digitalen Wandel

### **Zwischenfazit: In 6 Schritten zum digitalen Wandel**

#### **1. Schritt: Workshop**

- Unternehmen sollten als Erstes einen Workshop zu den Chancen des digitalen Wandels für die eigene Firma einberufen

#### **2. Schritt: Definition von Anwendungsfällen**

- Im Rahmen des Workshops identifizieren Unternehmen konkrete Anwendungsfälle (Use Cases) -> keep it simple

#### **3. Schritt: Priorisierung**

- In einem Workshop entstehen meist 5-7 Anwendungsszenarien, mit denen das Unternehmen seine Geschäftstätigkeit weiterentwickeln kann.

#### **4. Schritt: Realisierung von erfolgsversprechenden Kurzprojekten**

- Im Zuge dieser Priorisierung kristallisieren sich die Use Cases heraus, die das Unternehmen vergleichsweise einfach und schnell testen („explorativ“) und adaptieren kann.

#### **5. Schritt: Interne Vermarktung der Erfolge**

- Die ersten Erfolge sind im besten Fall ein interner Weckruf

#### **6. Schritt: Realisierung grundlegender Projekte**

- Projekte angehen, die seine Durchschlagskraft am Markt verbessern.

## 2.8 Schlüsselkennzahlen

### **Was sind Ihre digitalen Schlüssel-Kennzahlen?**

Community	Partner	Portfolio	Ressourcen
<ul style="list-style-type: none"> <li>• Reichweite</li> <li>• Unique Users/Visitors</li> <li>• Conversion Rate</li> <li>• Cost per Click (CPC)</li> <li>• Customer Lifetime Value</li> </ul>	<ul style="list-style-type: none"> <li>• Mitarbeiterfluktuation</li> <li>• Ideenvorschläge pro Mitarbeiter</li> <li>• Bewerbungsquote bei Business Model Wettbewerben</li> <li>• Projektkosten</li> </ul>	<ul style="list-style-type: none"> <li>• Marktwachstum</li> <li>• Marktanteil</li> <li>• Abschreibungen auf Firmenwert</li> <li>• Digitale Abonnements</li> <li>• Abo-Kündigungen</li> </ul>	<ul style="list-style-type: none"> <li>• Anteil Digitalumsatz</li> <li>• Online-Werbeumsatz</li> <li>• EBITDA (analog/digital)</li> <li>• ROI/Payback auf Inkubationsausgaben</li> </ul>

## 2.9 Fazit

### 2.9.1 Kritik und Ausblick

#### Kritik und Ausblick

Die Digitalisierung wird diskutiert und kritisiert, und insbesondere die nächste Entwicklungsstufe, die sie ermöglicht, ist in Gesellschaft, Wirtschaft und Politik umstritten. Die Bereichsethiken können die bei der Digitalisierung entstehenden moralischen Probleme – etwa in Bezug auf die Industrie 4.0 – reflektieren, allen voran Technik-, Informations- und Wirtschaftsethik.

**Technik- und Informationsethik** fragen nach dem Zugewinn und dem Verlust der persönlichen und informationellen Autonomie und nach der Abhängigkeit der Kunden von IT und IT-Unternehmen, die Teildisziplinen der **Wirtschaftsethik** nach der Verantwortung der Unternehmen (Unternehmensexethik) bei der Datennutzung und bei Fertigungsprozessen gegenüber Benutzern und Mitarbeitern und nach der Verantwortung der Konsumenten digitaler Güter und Dienstleistungen (**Konsumentenethik**). Mit den Folgen befassen sich auch Rechtswissenschaft, Medizin, Soziologie und Psychologie. [...] Vor dem Hintergrund, dass Arbeiter und Angestellte ihre Arbeit verlieren, weil Hard- und Softwarearbeiter diese günstiger und schneller (manchmal auch besser) verrichten, widmet man sich Ansätzen und Konzepten wie der Robotersteuer und dem bedingungslosen Grundeinkommen und denkt über Faktoren nach, die die soziale Gerechtigkeit und den gesellschaftlichen Zusammenhalt fördern.

Folie 28, 09.03.2017

Quelle: <http://wirtschaftslexikon.gabler.de/Definition/digitalisierung.html>

### 2.9.2 Handlungsempfehlung

- Sehen Sie neue **Technologien** als **Chance** für Ihr Unternehmen, nicht als Bedrohung.
- Brechen Sie klassische Unternehmensstrukturen auf und finden Sie **neue Strategien** für Ihr Unternehmen.
- Denken Sie Digitalisierung vom **Kunden** her, und überlegen Sie sich, welchen Mehrwert Sie Ihrer Zielgruppe bieten sollte.
- Definieren Sie **Rollen im Unternehmen** neu, um eine erfolgreiche digitale Transformation zu ermöglichen.
- Ermitteln Sie die **wichtigsten Kanäle**, auf denen Ihre Zielgruppe unterwegs ist, und bieten Sie an jedem Touchpoint eine persönliche Kommunikation in Echtzeit.
- Lassen Sie in Ihren Überlegungen den Einfluss auf die Gesellschaft nicht ausser acht.

## 2.9.3 Zusammenfassung

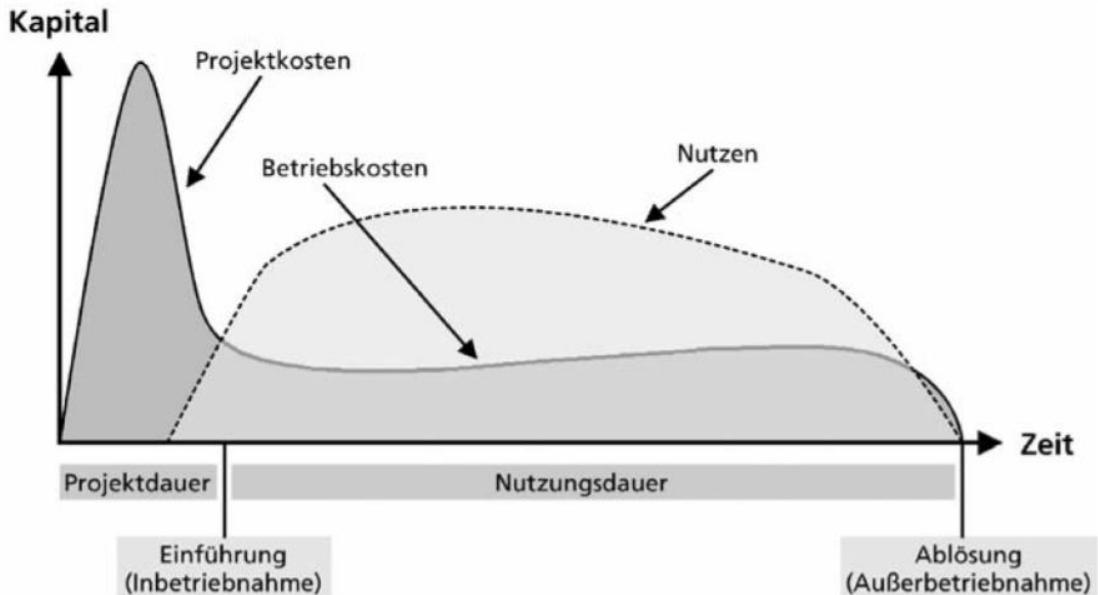
### Zusammenfassung: Chancen und Risiken der Digitalisierung für das KMU

Risiken	Chancen												
 <p>Kanton Genf verbietet Fahrdienst Uber Schweizer Taxifahrer demonstrieren gegen Uber «Wenn nötig, streiken wir»</p> <p><b>SPIEGELON</b> «Wir sind keine Dinosaurier!»</p> <p>Occupation Number of Workers</p> <table border="1"> <tbody> <tr> <td>Transportation</td> <td>3,628,000</td> </tr> <tr> <td>Retail salespersons</td> <td>3,286,000</td> </tr> <tr> <td>First line supervisors</td> <td>3,132,000</td> </tr> <tr> <td>Cashiers</td> <td>3,109,000</td> </tr> <tr> <td>Secretaries</td> <td>3,082,000</td> </tr> <tr> <td>Managers, all other</td> <td>2,898,000</td> </tr> </tbody> </table> <p>Automatisierungsprognosen 2025</p>	Transportation	3,628,000	Retail salespersons	3,286,000	First line supervisors	3,132,000	Cashiers	3,109,000	Secretaries	3,082,000	Managers, all other	2,898,000	 <p>According to Uber CEO Travis Kalanick, who spoke at the DLD Conference in Munich on Sunday, the taxi market in San Francisco is about \$140 million per year. Uber's revenues in San Francisco, meanwhile, are running at \$500 million per year. That's more than three times the size of the taxi market.</p> <p>Markt für Taxidienstleistungen nimmt um Faktor 3 zu</p>  <p>Wielandbus AG hat 3 neue Fotos hinzugefügt. Wir sind dabei: Die neue Mobilitäts-App der Schweiz. Als Partner und als erstes Unternehmen in der Westschweiz. Taxifahren ganz einfach zu Fixpreisen. GO - so einfach geht Taxi.</p>
Transportation	3,628,000												
Retail salespersons	3,286,000												
First line supervisors	3,132,000												
Cashiers	3,109,000												
Secretaries	3,082,000												
Managers, all other	2,898,000												
<b>Folien 26-28</b> <b>«Take Away» Messages:</b> <ul style="list-style-type: none"> <li>Gleich lange Spieße, Gesetzgeber hinkt der Entwicklung hinterher</li> <li>Ethische Aspekte für Gesellschaft mitberücksichtigen!</li> </ul>	<b>Folien 4-9</b> <b>«Take Away» Messages:</b> <ul style="list-style-type: none"> <li>Ansatzpunkte für Digitalisierung: Prozesse, Services, Produkte, disruptive Geschäftsmodelle</li> <li>Geschwindigkeit &amp; Exploration</li> </ul>	<b>Folien 10-20</b> <b>«Take Away» Messages:</b> <ul style="list-style-type: none"> <li>Chancen entlang des gewandelten Kundenbedürfnis («Customer Journey»)</li> <li>Potential der neuen Technologien</li> <li>Neue Denkmuster im digitalen Wandel</li> </ul>											

### 3 Wirtschaftlichkeitsanalyse

#### 3.1 Kosten und Nutzen bestimmten den Wertbeitrag der IT

##### **Kosten und Nutzen bestimmen den Wertbeitrag der IT**

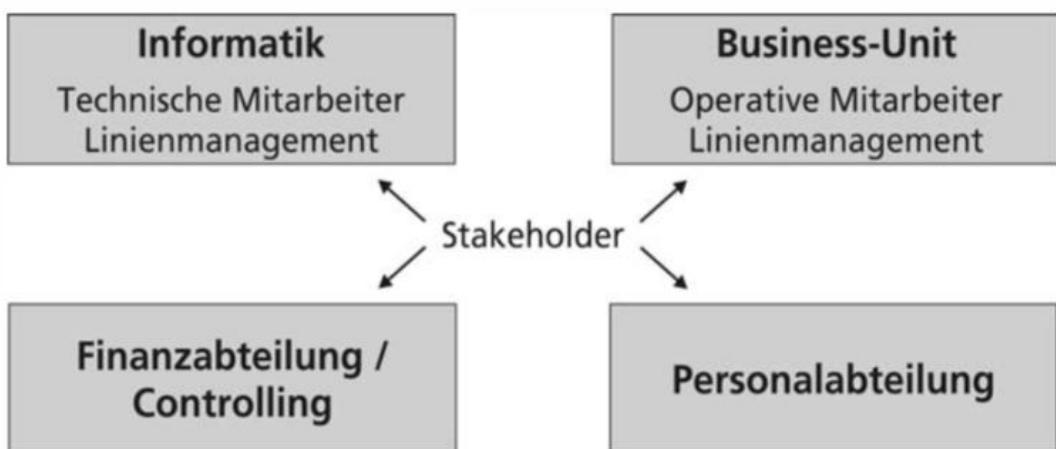


#### 3.2 Business Case

##### 3.2.1 Definition

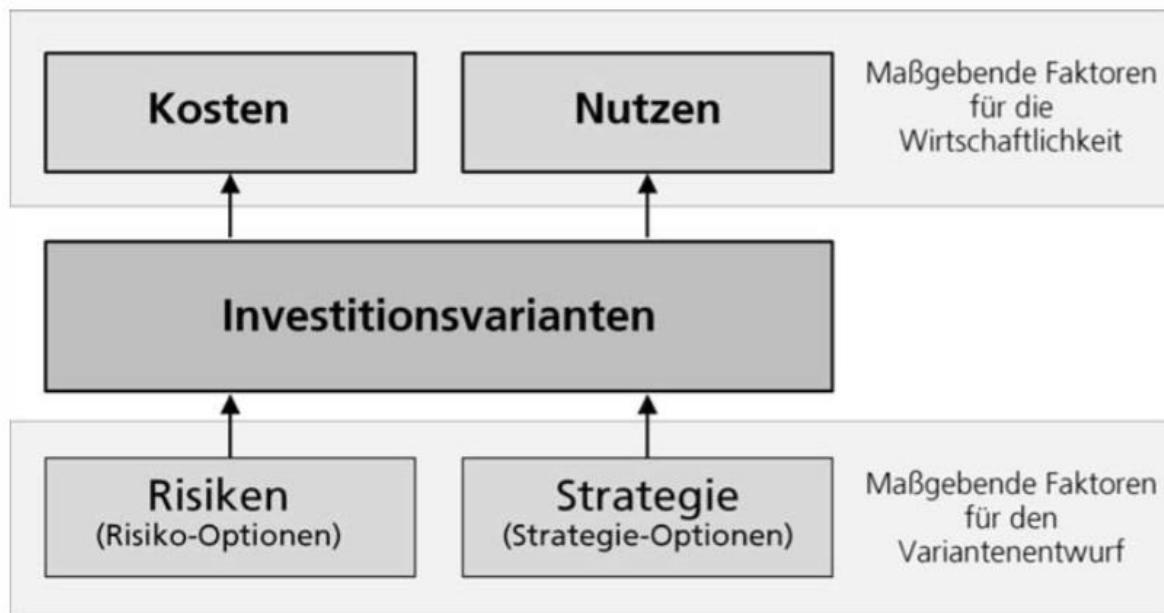
Ein Business Case fasst alle entscheidungsrelevanten Aspekte eines geplanten Vorhabens mit dem Ziel zusammen, die wirtschaftliche Vorteilhaftigkeit und strategische Konformität des Gesamtprojekts aufzuzeigen und eine abschliessende Management-Entscheidung über dessen Ausführung zu ermöglichen.

##### 3.2.2 Stakeholder



### 3.2.3 Bausteine

## Bausteine eines Business Cases



### 3.2.4 Investitionsentscheidung

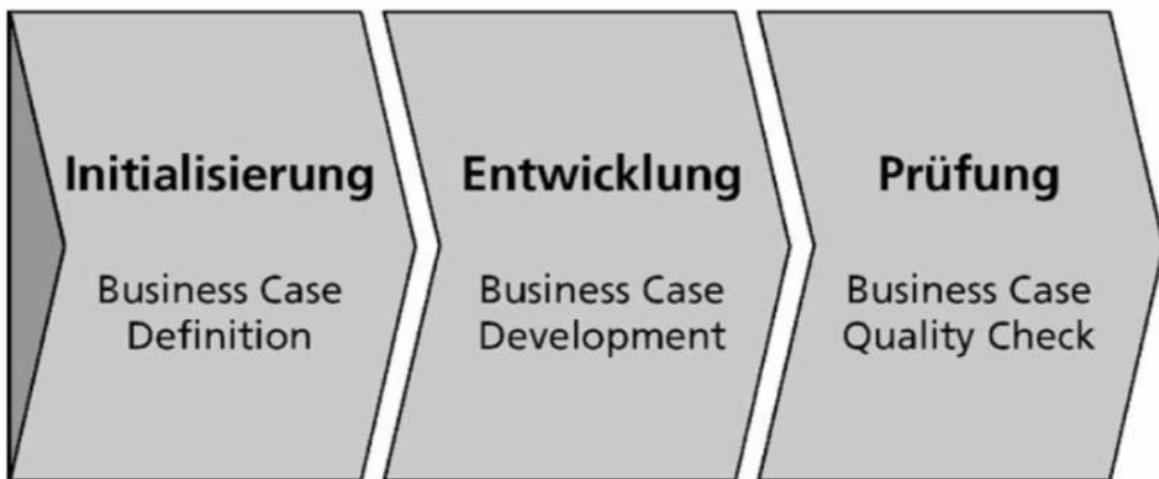
## Facetten der Investitionsentscheidung

Durchführungsentscheidung	Auswahlentscheidung
Absolute Vorteilhaftigkeit	Relative Vorteilhaftigkeit
<p>Soll über eine einzige Investition entschieden werden, so wird im Rahmen der Business-Case-Erstellung die Vorteilhaftigkeit im Sinne einer Ja-/Nein-Entscheidung ermittelt.</p> <p>Die Kernfrage lautet: Ist das zur Entscheidung anstehende Projekt vorteilhaft oder nicht?</p>	<p>Stehen mehrere miteinander konkurrierende Projektvorschläge zur Disposition, so wird anhand von Business Cases deutlich, welches der Investitionskandidaten das wirtschaftlichste Vorhaben ist.</p> <p>Ein analoges Problem besteht bei der Planung des optimalen Investitionsprogramms. Die zu prüfenden Projekte schließen sich nicht gegenseitig aus. Die Bestimmung der relativen Vorteilhaftigkeit unterstützt die Priorisierung.</p> <p>Die Kernfrage lautet in beiden Fällen: Welche Investitionsalternative ist vorteilhafter?</p>

### 3.3 Business-Case-Erstellung

#### 3.3.1 3 Phasen

## Die drei Phasen der Business-Case-Erstellung



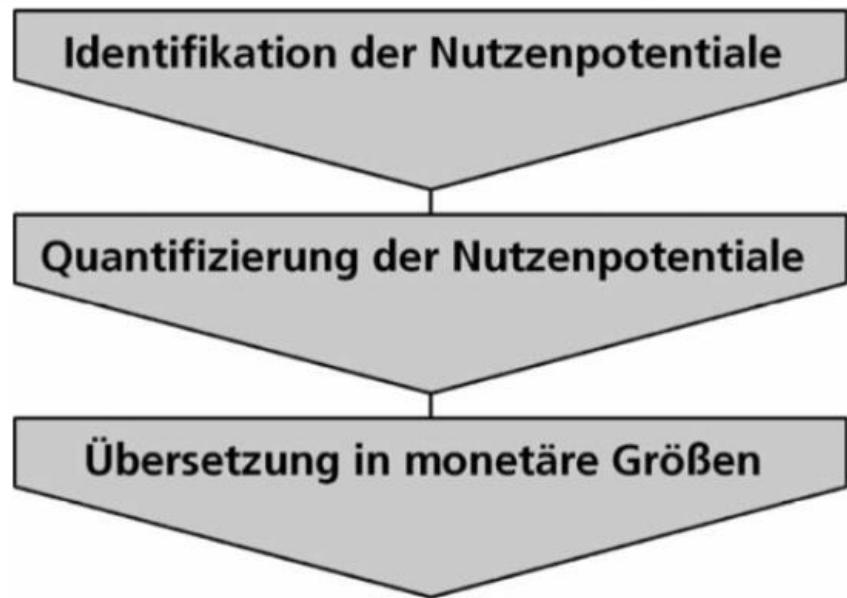
#### 3.3.2 Vorgehensmodell

## Vorgehensmodell für einen Business Case



### 3.3.3 Nutzenfestlegen

## Prozess zur Festlegung des Nutzens



### 3.3.4 Dokumentation

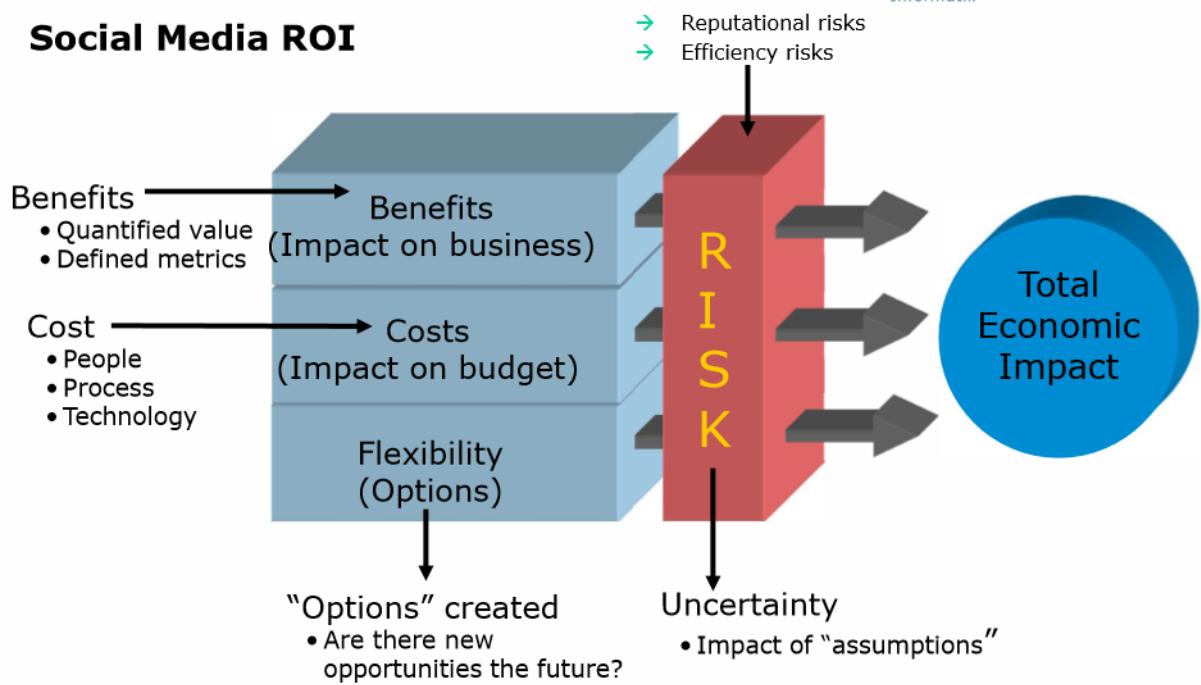
## Aufbau einer Business Case Dokumentation

Business Case – Projekt „XY“

1. Management Summary
2. Projektvorstellung
  - 2.1 Anliegen (Problem / Opportunität)
  - 2.2 Projektziel (Projektvision)
  - 2.3 Ausgangslage (Beschreibung der gegenwärtigen Situation)
  - 2.4 Anforderungen an die Lösungsumsetzung und Zielsituation
  - 2.5 Zielsituation (Beschreibung des angestrebten Zustands)
  - 2.6 Projektplan-Übersicht (Etappen, Termine, Personalaufwand)
  - 2.7 Alternativen
  - 2.8 Risiken
3. Wirtschaftlichkeitsnachweis
  - 3.1 Grundlagen
  - 3.2 Nutzen
  - 3.3 Kosten
  - 3.4 Wirtschaftlichkeitsberechnung
  - 3.5 Schlussfolgerungen
4. Projektdetails
  - 4.1 Projektorganisation
  - 4.2 Projektplan (detailliert)
  - 4.3 Kritische Erfolgsfaktoren
  - 4.4 Kriterien für die Erfolgsmessung (Performance Measures)

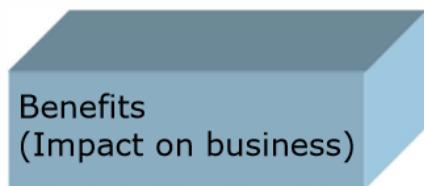
### 3.4 Social Media Business Case → Kunden Community

#### 3.4.1 Return of Investment



#### 3.4.2 Nutzen

##### Examples of benefits



- Cost savings
  - Reduce call volume
  - Reduce email volume
  - Increase agent productivity
  - Better FCR (first contact resolution)
  - Reduce SEO costs
- Revenue improvements
  - Increase customer lifetime value
  - Increase product ideation
  - Increase lead conversion rates

### 3.4.3 Nutzenkategorien

#### **Vielfältige Nutzenkategorien**

- Kunden lösen die Probleme anderer Kunden
- Weniger oder kaum Interaktionen mit dem Unternehmen.
  - Kunden lesen die Posts
  - Weniger Anrufe ins Contact Center
- Und die Agenten nutzen die KM Community ebenfalls
  - Reduzierte Lösungszeiten
  - Qualitativ und inhaltlich bessere Antworten.

### 3.4.4 Erstlösungsquote

#### **Erstlösungsquote erhöht sich**

- Die Erstlösungsquote beeinflusst
  - Kundenzufriedenheit
  - Wiederkaufwahrscheinlichkeit/Vertragsverlängerung
  - Gute Mund-zu-Mund Propaganda
  - Aber auch die Kosten, denn:

DER KUNDE RUFT NUR  
EINMAL AN!

### 3.4.5 Weitere Nutzenkategorien

**Ok, für den Service soweit verstanden, aber: Wie rechnet man die Nutzenkategorien für den Rest der Firma?**

#### Product Development

- Neue Ideen aus der Kundencommunity
- Neue Ideen für die Antworten an Kunden



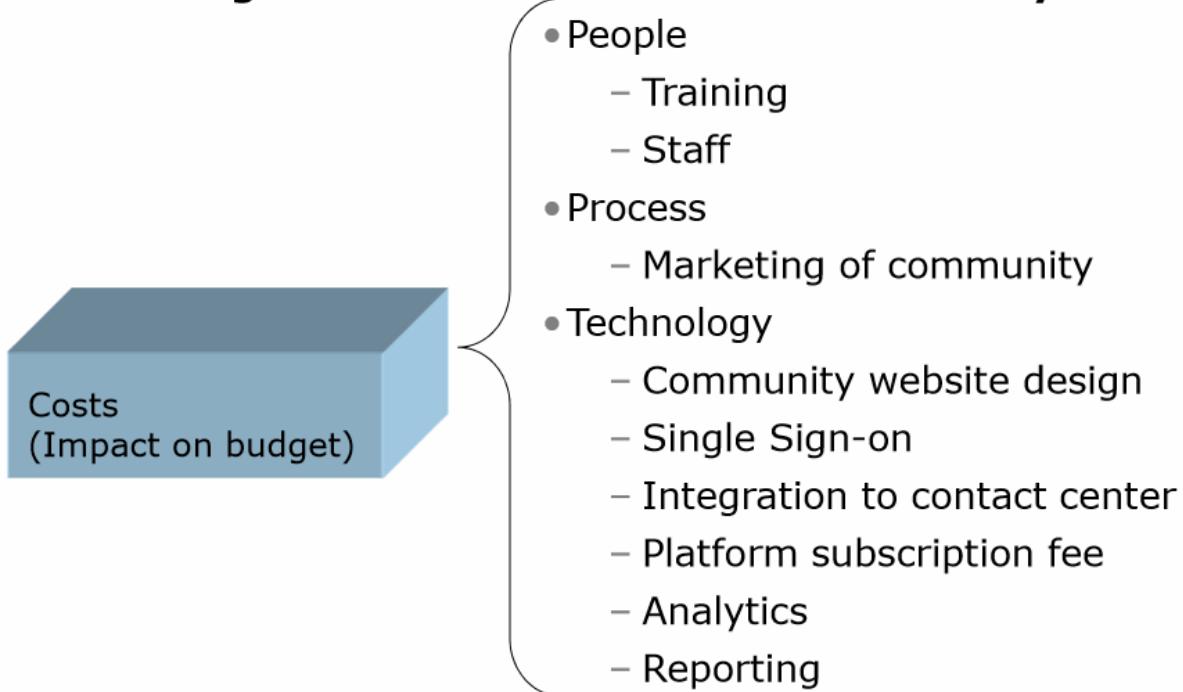
#### Marketing und Sales

- Werbung für das erste Produkt, welches durch den Input der Kunden entstanden ist.

### 3.5 Online Kunden-Community Allgemein

#### 3.5.1 Kostenkategorien einer Online Kunden-Community

#### **Kostenkategorien einer Online Kunden-Community:**



#### 3.5.2 Initialkosten

#### **Initialkosten von Kunden-Communities**

Project phase	Key costs
Start-up: technology	<ul style="list-style-type: none"><li>• Creating the skin for community to match the corporate Web site</li><li>• Creating a user registration and sign-in procedure</li><li>• Connecting the agent desktop and the knowledge management system to the company's Web site and community</li><li>• Evaluating and improving knowledge management and search capabilities</li><li>• Integrating the community so that marketing has access to the community and can participate</li><li>• Integrating the community so that sales has access to the community and can participate</li></ul>
Start-up: people	<ul style="list-style-type: none"><li>• Project manager who oversees the community project</li><li>• Community manager who is the operational owner of the community</li><li>• IT resources that oversee and coordinate the integration with the company's IT infrastructure and systems</li><li>• Training for key personal in community best practices</li></ul>
Start-up: process	<ul style="list-style-type: none"><li>• Marketing and launch promotion for the community</li><li>• Creating the community plan and developing community policies</li></ul>

### 3.5.3 Wiederkehrende Kosten

## **Wiederkehrende Kosten von Kunden-Communities**

Recurring: technology	<ul style="list-style-type: none"><li>• Yearly license fee for a leased platform (SaaS model)</li><li>• Analytics package to measure key performance metrics</li><li>• Reporting capability for analytics</li></ul>
Recurring: people	<ul style="list-style-type: none"><li>• Community moderator</li><li>• Community owner who is the operational owner of community</li><li>• IT resources for ongoing IT infrastructure support</li><li>• Knowledge management manager to update KM content</li></ul>
Recurring: process	<ul style="list-style-type: none"><li>• Ongoing marketing and promotion to continuously engage super users and community members</li></ul>

### 3.6 Kennzahlen

## **Die wichtigsten Kennzahlen**

### - **NPV:** Net Present Value

Diskontierung von Kosten und Nutzen  
Differenz über Betrachtungsdauer

«Was bleibt nach Abschluss der Betrachtungsdauer»

### - **ROI:** Return of Investment

Diskontierung von Kosten und Nutzen  
$$\text{ROI} = (\text{Total diskontierter Nutzen} - \text{Total diskontierte Kosten}) / \text{Total diskontierter Kosten}$$

«Was erhalte ich für mein eingesetztes Kapital zurück in %»

### - **Pay Back/Break Even**

«In welchem Jahr komme ich in die Gewinnzone»

### 3.6.1 Diskontierung

#### **Einschub Diskontierung**

= Abzinsung (mit einem Prozentsatz) «alternativer Einsatz des Geldes»  
Zinsenzinsberechnung

Diskontierungssatz: 8%

Diskontierfaktor

	0.93	0.86	0.79
--	------	------	------

Jahr

1	2	3	Total
---	---	---	-------

Nutzen	100	100	100	300
diskontierter Nutzen	93	86	79	258

Analog mit Kosten

### 3.6.2 Berechnungsbeispiele

#### **Beispiel für die Berechnung der Kennzahlen zweier Projekte NPV, ROI, Payback**

Diskontiersatz	8%							
Diskontierfaktor	0.93	0.86	0.79	0.74				
					Jahr			
<b>Projekt 1</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>		<b>Total</b>		
Kosten	100'000	25'000	25'000	25'000	175'000			
diskontierte Kosten	92'593	21'433	19'846	18'376	152'248			
Nutzen	0	80'000	80'000	80'000	240'000	NPV	38'648	
diskontierter Nutzen	0	68'587	63'507	58'802	190'896	ROI	25%	
						Payback	Jahr 4	
disk. Nutzen - disk. Kosten	-92'593	47'154	43'661	40'427	38'648			
kum. disk. Nutzen - disk. Kosten	-92'593	-45'439	-1'778	38'648				
					Jahr			
<b>Projekt 2</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>Total</b>			
Kosten	15'000	61'000	50'000	50'000	176'000			
diskontierte Kosten	13'889	52'298	39'692	36'751	142'630			
Nutzen	10'000	60'000	65'000	75'000	210'000	NPV	24'796	
diskontierter Nutzen	9'259	51'440	51'599	55'127	167'426	ROI	17%	
						Payback	Jahr 3	
disk. Nutzen - disk. Kosten	-4'630	-857	11'907	18'376	24'796			
kum. disk. Nutzen - disk. Kosten	-4'630	-5'487	6'421	24'796				

### 3.6.3 ROI

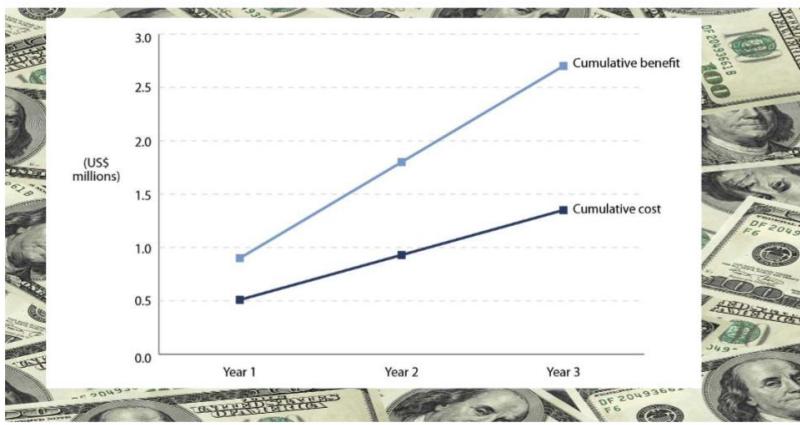
## Der ROI Business Case: Benefit – Kosten und dann abzinsen!

	Year 1	Year 2	Year 3	Total	Present Value (PV)
Benefit	\$904,400	\$904,400	\$904,400	\$2,713,200	\$2,330,727
Cost	\$516,060	\$418,310	\$418,310	\$1,352,681	\$1,168,535
Net cash flow	\$388,340	\$486,090	\$486,090	\$1,360,519	\$1,162,191
NPV	\$1,162,191				
ROI	99%				
Payback	< 12 months				



### 3.7 Fazit

Gesamthaft lässt sich ein Business Case folgendermassen darstellen:



## Zusammenfassung «Wirtschaftlichkeitsanalyse»

- Sie kennen die Einsatzmöglichkeiten/Bedeutung von Business-Cases.
- Sie kennen die wichtigsten Elemente die ein Business-Case abdecken sollte.
- Sie sind mit dem Vorgehen bei der Erstellung eines Business-Cases vertraut.
- Sie kennen die wichtigsten finanziellen Kennzahlen eines Business Cases und wie sie diese im Rahmen einer Wirtschaftlichkeitsbetrachtung über die Nutzungsdauer der Investition ermitteln können.

## 4 Outsourcing

### 4.1 Begriffsdefinition

- Der Begriff „**Outsourcing**“ ist ein Kunstwort aus den Worten „**Outside**“, „**Resource**“ und „**Using**“.
- IT-Outsourcing ist die mittel- und langfristige **Übertragung** einzelner oder aller bisher innerbetrieblich erfüllten **IT-Aufgaben** an ein rechtlich unabhängiges Dienstleistungsunternehmen.
- Grundsätzlich wird das Verhältnis zwischen Dritten und der eigenen IT-Organisation ausschließlich durch **Verträge** und **Gesetze** geregelt.
- **Idee dahinter:** Ein Unternehmen soll sich auf seine Kernkompetenzen konzentrieren.

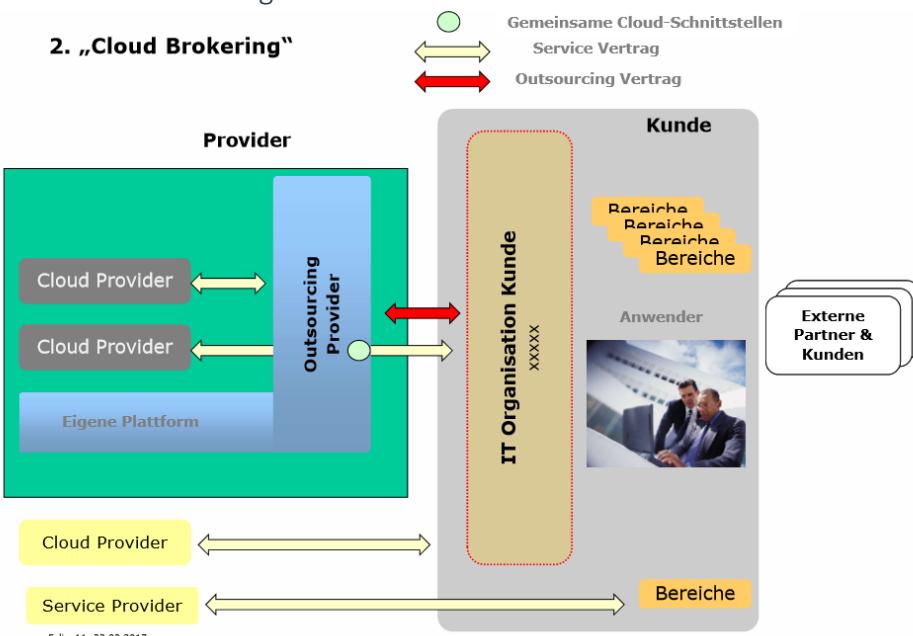
### 4.2 Markt

#### 4.2.1 Veränderungen im Service Einkauf

##### 2. Veränderung im Service Einkauf

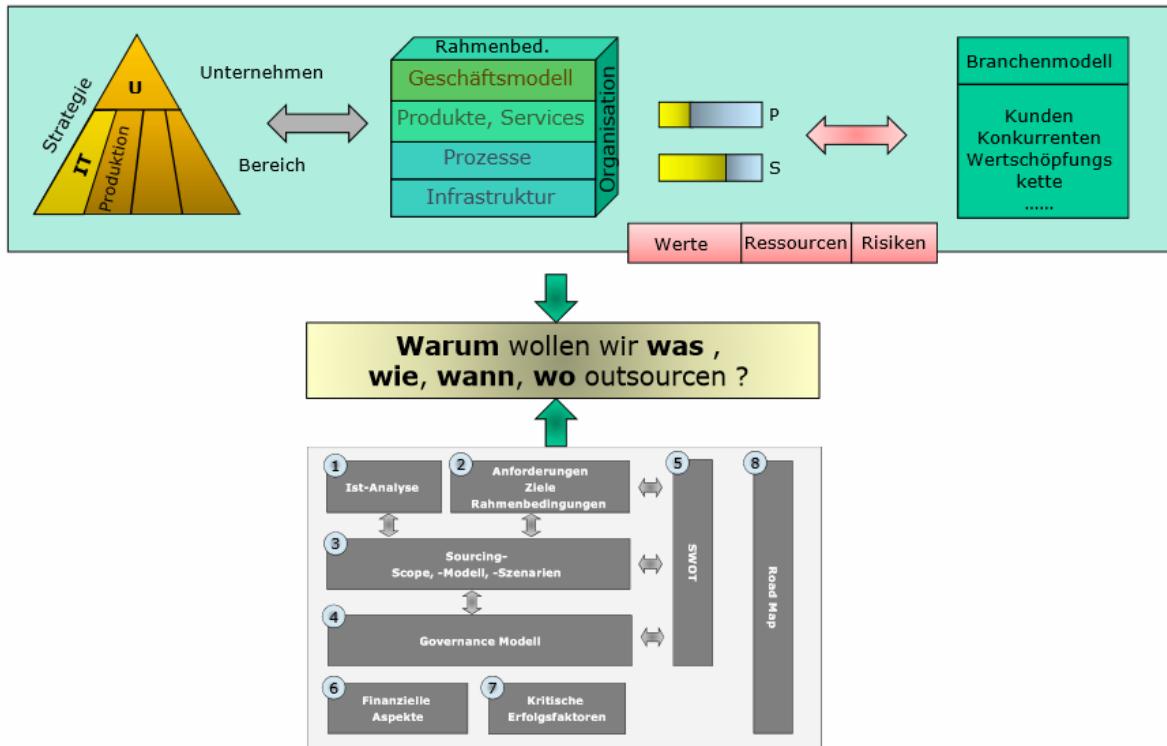
Veränderungen im Serviceeinkauf		
Kriterium	Klassisches Outsourcing	Cloud Computing
Services	Services sind auf Kunden abgestimmt	Services sind vom Provider standardisiert, industrialisiert, automatisiert und skalierbar
Service Level	Individuell	Provider bestimmt Standard
Technologie	Mitbestimmung durch Kunde	Provider bestimmt Standard
Releasemanagement	Mitbestimmung durch Kunde	Provider bestimmt Standard
Vertrag	Kunde gibt vor	Provider bestimmt Standard
Preismodelle	Kunde gibt vor	Provider bestimmt Standard
Standort der Daten	Mitbestimmung durch Kunde	Provider bestimmt Standard
Betreuung	Ansprechpartner	Selbstbedienung durch den Kunden über Web Portale

#### 4.2.2 Cloud Brokering



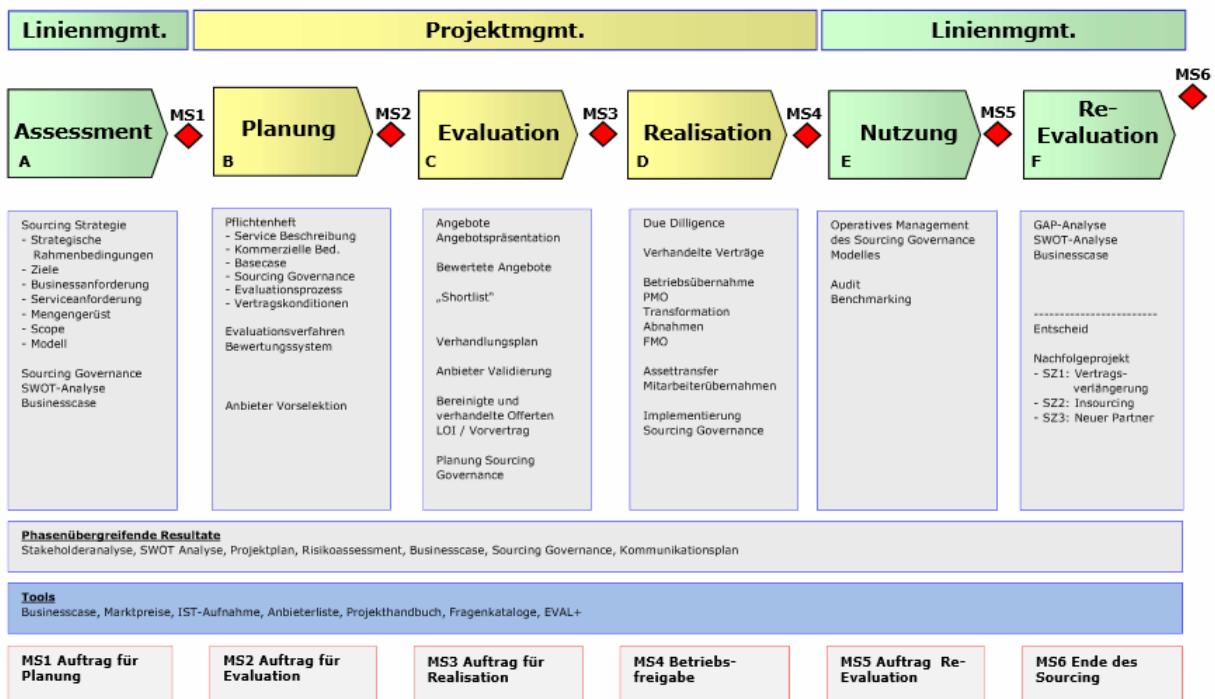
## 4.3 Strategie Modell

### **3. Strategie Modell**



### 4.3.1 Phasen Modell

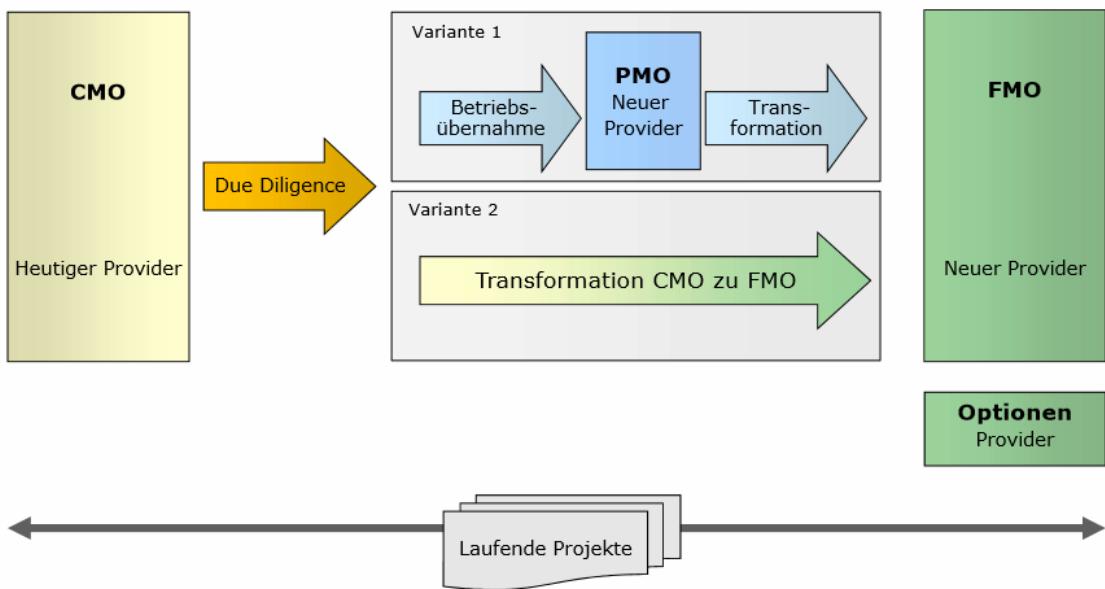
### **3. Phasen Modell (Soberano)**



#### 4.3.2 Vom CMO zum FMO

Informatik

### 3. Vom CMO zum FMO



CMO: Current Mode of Operation  
 PMO: Present Mode of Operation  
 FMO: Future Mode of Operation

#### 4.3.3 Typische Fragestellungen

### 3. Typische Fragestellungen

#### - Scope

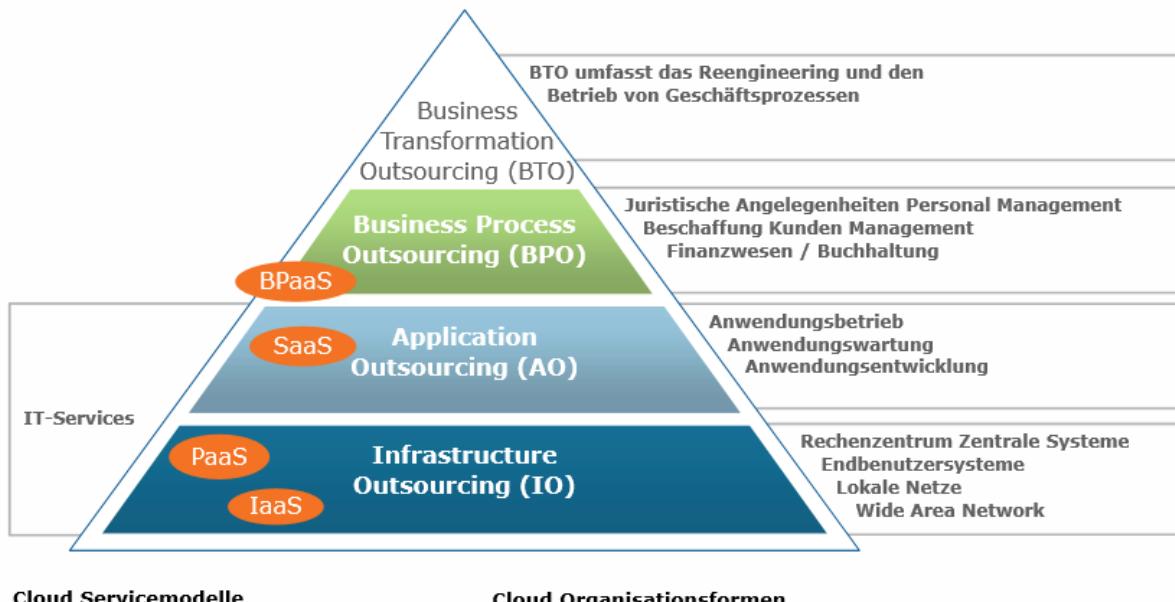
- Was sind die Kernkompetenzen und machen wir sie selber (welche Fertigungstiefe brauchen wir)?
- Wie können wir die Services bewerten?
- Was sind die Entscheidungskriterien für ein Outsourcing?

#### - Modell

- Wie wollen wir die zu beschaffenden Service bündeln (Servicepakete)?
- Wie viele Provider wollen wir und wie teilen wir die Services auf diese auf?
- Welches Kooperationsmodell wollen wir?
- Welche Vergütungsmodelle wollen wir pro Servicebündel?
- Was sind die Restriktionen betr. dem Ort der Leistungserbringungen?
- Welches Cloudmodell & Organisationsform bei welchen Services?
- Wie soll die Datenhaltung zusammen mit der Integration, Interoperabilität sichergestellt werden?
- Wer und wie soll das End To End Monitoring sicherstellen?
- Wer führt wie die Provider?

#### 4.3.4 Outsourcing Scope

### 3. Outsourcing Scope & Formen



#### Cloud Servicemodelle

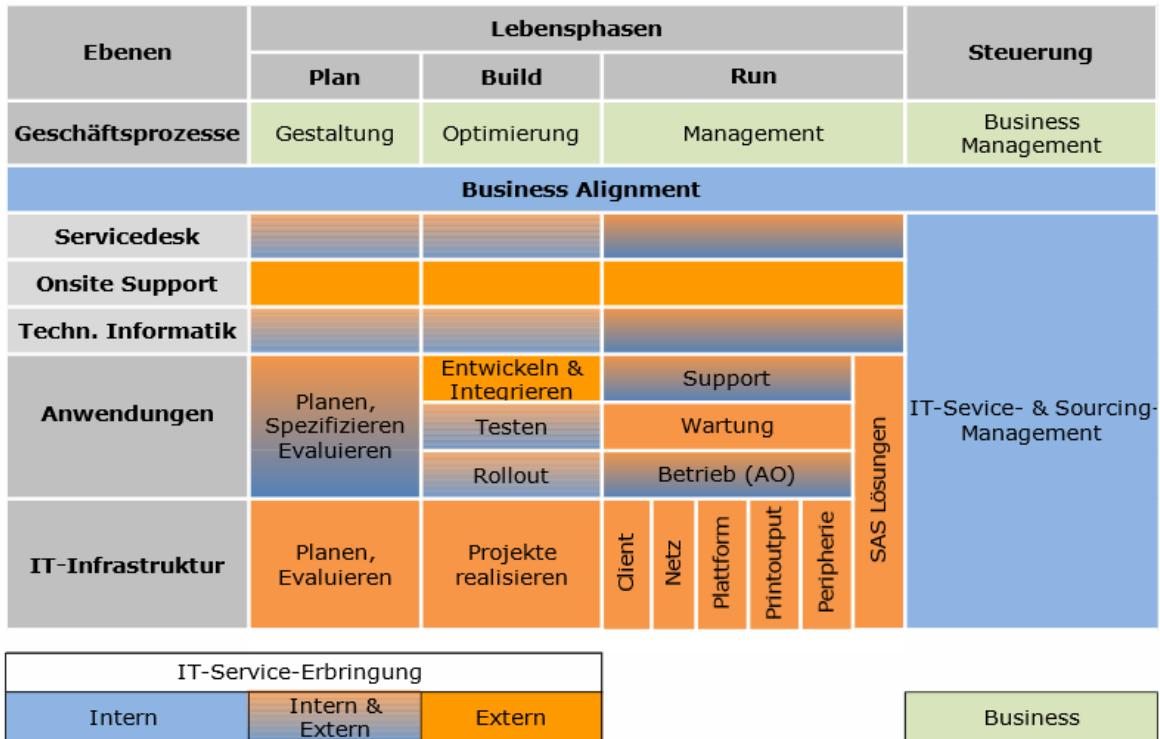
BPaaS: Business Process as a Service  
 SaaS: Software as a Service  
 PaaS: Platform as a Service  
 IaaS: Infrastructure as a Service

#### Cloud Organisationsformen

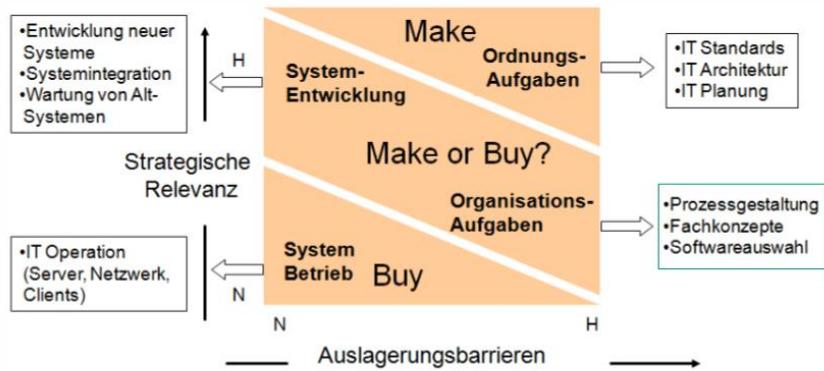
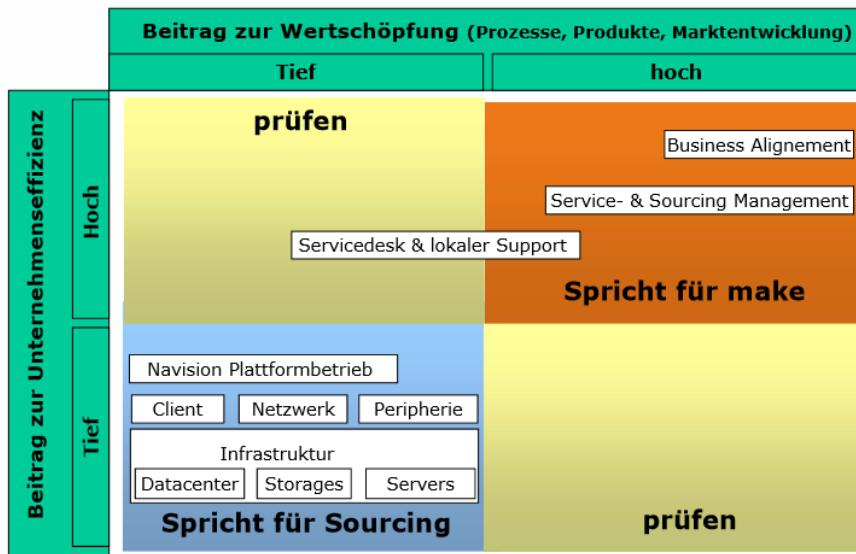
Private Cloud  
 Community Cloud  
 Public Cloud  
 Hybrid Cloud

#### 4.3.5 Sourcing Scope

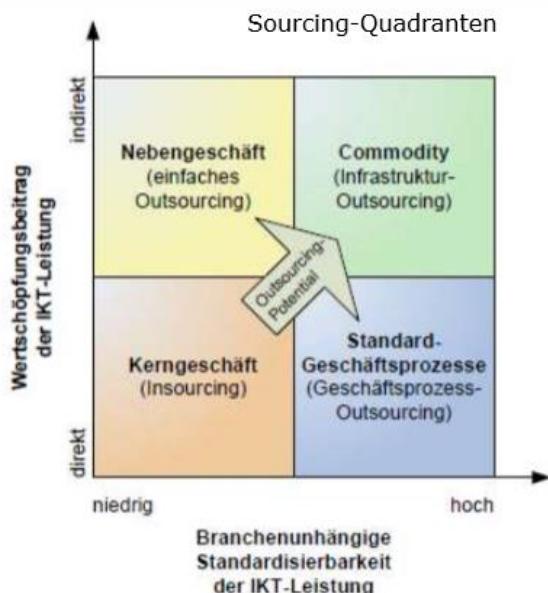
### 3. Sourcing Scope (plan, build, run)



#### 4.3.6 Bewertung

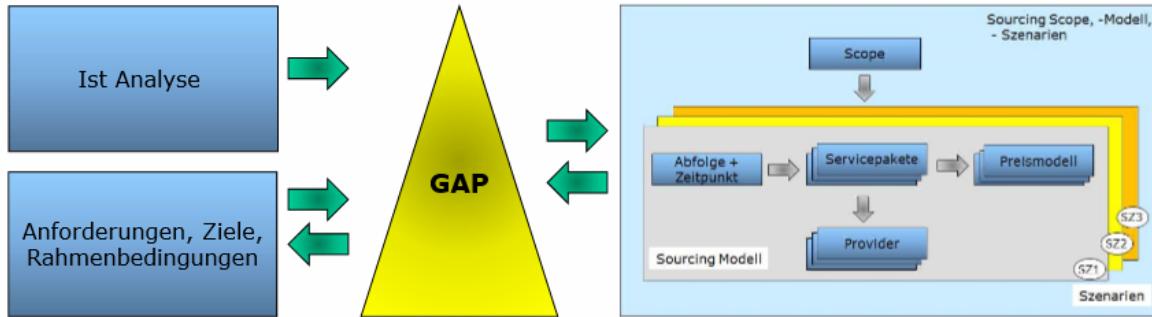


#### 4.3.7 Bewertung nach Baselstadt

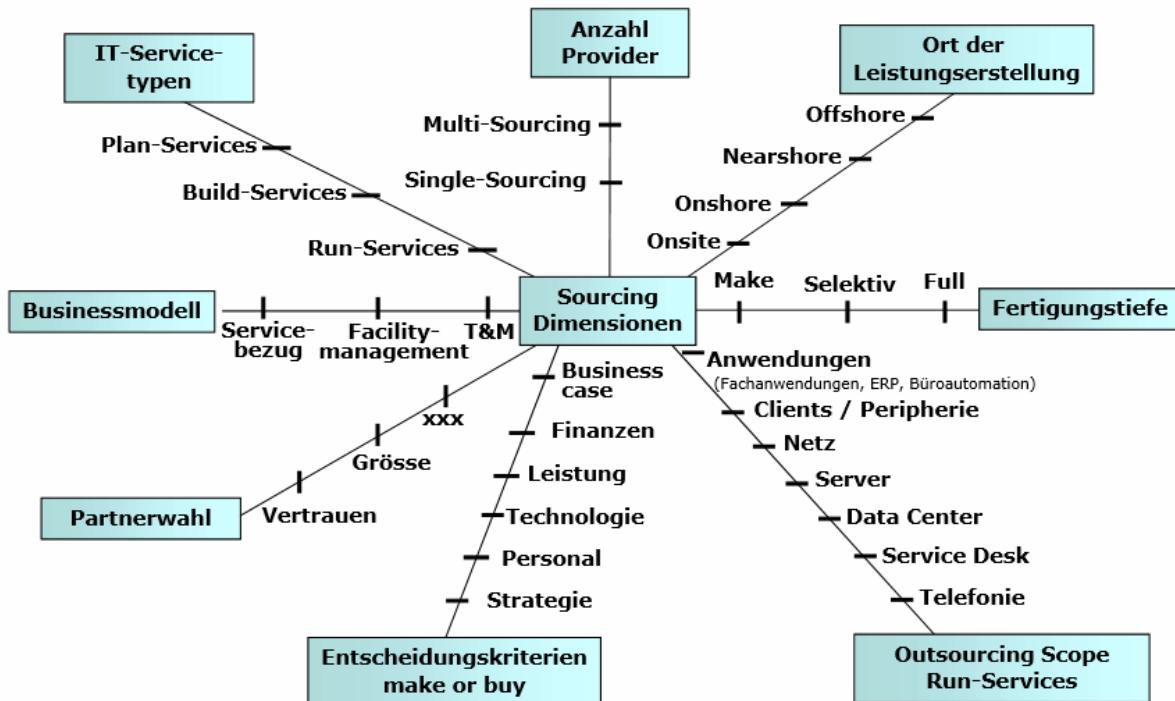


#### 4.3.8 Sourcing Scope, -Modell, -Szenarien

- Hier geht es darum die **strategischen Handlungsoptionen** in Form des Sourcing Scope, Sourcing Modell sowie der möglichen Sourcing Szenarien zu erarbeiten und zu bewerten.
- Dies ist ein interaktiver Prozess wie die Darstellung aufzeigt.
- Die nachfolgenden Modelle bieten dazu praxiserprobte, effektive und effiziente Werkzeuge dazu.



#### 4.3.9 Sourcing Prinzipien



## 4.4 Argument-Bilanz

### 4.4.1 Strategie

<b>1. Strategie</b>	
<b>PRO</b>	<b>CONTRA</b>
<ul style="list-style-type: none"> <li>• Konzentration auf das Kerngeschäft</li> <li>• Konzentration auf strategisch wichtige Fach- und IT-Aufgaben</li> <li>• Vorteile überschaubarer, schlanker, flexibler Organisationen</li> <li>• Kooperationen in strategischen Allianzen statt vertikaler Hierarchien</li> <li>• Beschleunigte Umsetzung von Reengineering-Erkenntnissen</li> <li>• Auf neuestem Technik-Stand befindliche, innovative IT-Lösungen</li> <li>• Standardisierung der eingesetzten IT-Systeme</li> <li>• Verbesserte Führbarkeit des IT-Bereiches</li> <li>• Reduktion des Risikos der Erfüllung von IT-Aufgaben</li> </ul>	<ul style="list-style-type: none"> <li>• Verlust von IT-Know-how</li> <li>• Wettbewerbsrelevanz bestimmter IT-Aufgaben</li> <li>• Entstehen irreversibler Abhängigkeiten</li> <li>• Störung zusammengehöriger Prozesse</li> <li>• Vertraulichkeit von Geschäftsprozessen und -daten</li> <li>• Risiken aus der Zusammenarbeit</li> <li>• Starke Machtposition des Outsourcing-Dienstleisters bei Realisierung von Individuelllösungen durch Wissensmonopole</li> <li>• Unterschiedliche Unternehmenskulturen</li> <li>• Probleme gegen Ende der Vertragslaufzeit</li> </ul>

### 4.4.2 Leistung

<b>2. Leistung</b>	
<b>PRO</b>	<b>CONTRA</b>
<ul style="list-style-type: none"> <li>• Hohe, vielfältige Kompetenz des Dienstleistungsunternehmens</li> <li>• Fachkundige Investitions- und Katastrophenplanung</li> <li>• Rasche Verfügbarkeit von Kapazitäten</li> <li>• Erhöhung der Betriebssicherheit</li> <li>• Zugang zu intern fehlendem IT-Know-how</li> <li>• Nutzung der Erfahrungen von Outsourcing-Dienstleistern bei Konversionen und Konsolidierungen</li> <li>• Sicherstellung des betrieblich notwendigen Angebots an IT-Lösungen</li> <li>• Klar definierte Leistungen und Verantwortlichkeiten</li> </ul>	<ul style="list-style-type: none"> <li>• Unrealistische Aussagen der Anbieter</li> <li>• Übervorteilung des Outsourcing-Nachfragers durch Informationsdefizite bei Vertragsgestaltung</li> <li>• Mangelnde Transparenz bezüglich (zu geringen) Umfangs der vertraglich vereinbarten Leistungen</li> <li>• Unzureichende Messbarkeit der Vertragserfüllung</li> <li>• Mangelnde Flexibilität der Verträge</li> <li>• Notwendigkeit zur Überwindung räumlicher Distanzen</li> <li>• Weniger informelle Kommunikation</li> <li>• Beeinträchtigung des Datenschutzes</li> <li>• Mangelnde Akzeptanz in Fachbereichen wegen fehlender Anwendernähe</li> </ul>

### 4.4.3 Kosten

<ul style="list-style-type: none"> <li>• Kostenreduktion im laufenden Betrieb</li> <li>• Wissensbasierte "Economies of Scale"</li> <li>• Bessere Verhandlungsposition gegenüber Anbietern von IT-Systemen</li> <li>• Bei entsprechender Vertragsgestaltung variable statt fixer Kosten</li> <li>• Gute Transparenz und Planbarkeit</li> <li>• Präzisere Leistungsverrechnung</li> </ul>	<ul style="list-style-type: none"> <li>• Transaktionskosten</li> <li>• Koordinationskosten</li> <li>• Probleme bei Softwarelizenzen</li> <li>• Bezugsgrößenbestimmung für Entgelt</li> <li>• Steigende Telekommunikationskosten</li> </ul>
---	--

### 4.4.4 Personal

<b>4. Personal</b>	
<b>PRO</b>	<b>CONTRA</b>
<ul style="list-style-type: none"> <li>• Mittelfristige Reduzierung der IT-spezifischen Probleme im Personalwesen</li> <li>• Job enrichment und Job enlargement für zum Outsourcing-Anbieter wechselndes IT-Personal</li> <li>• Raschere Verfügbarkeit von IT-Spezialisten</li> <li>• Verfügbarkeit interner IT-Mitarbeiter für innerbetrieblich verbleibende IT-Aufgaben</li> </ul>	<ul style="list-style-type: none"> <li>• Arbeitsrechtliche Probleme</li> <li>• Personalwiderstände</li> <li>• Motivationsprobleme</li> </ul>

#### 4.4.5 Finanzen

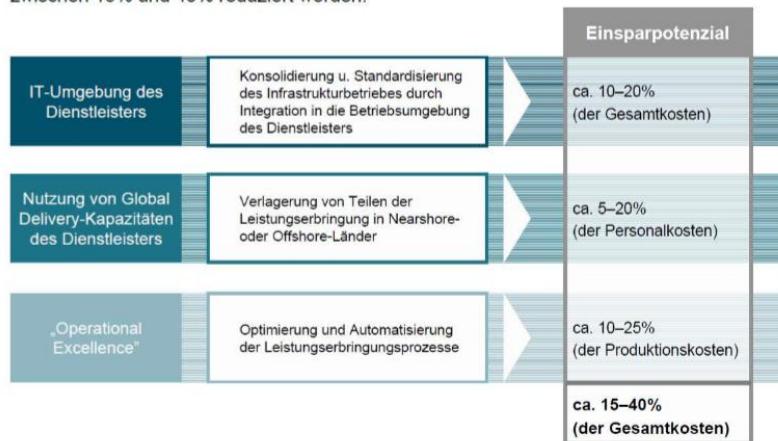
<b>5. Finanzen</b>	
<b>PRO</b>	<b>CONTRA</b>
<ul style="list-style-type: none"> <li>• Finanzmittelbeschaffung</li> <li>• Glättung der IT-Ausgaben</li> <li>• Auswirkungen auf Jahresabschluss und auf Steuerbelastung</li> <li>• Erfolgsbeteiligung des Dienstleisters möglich</li> </ul>	<ul style="list-style-type: none"> <li>• Abfindungen ausscheidender Mitarbeiter (Sozialplan)</li> <li>• Langfristig schlecht vorhersehbare Entgeltgestaltung</li> <li>• Negative Auswirkungen bei schwerwiegenden wirtschaftlichen Problemen des Outsourcing-Anbieters</li> </ul>

#### 4.5 Business-Case

##### 4.5.1 Kostensenkung

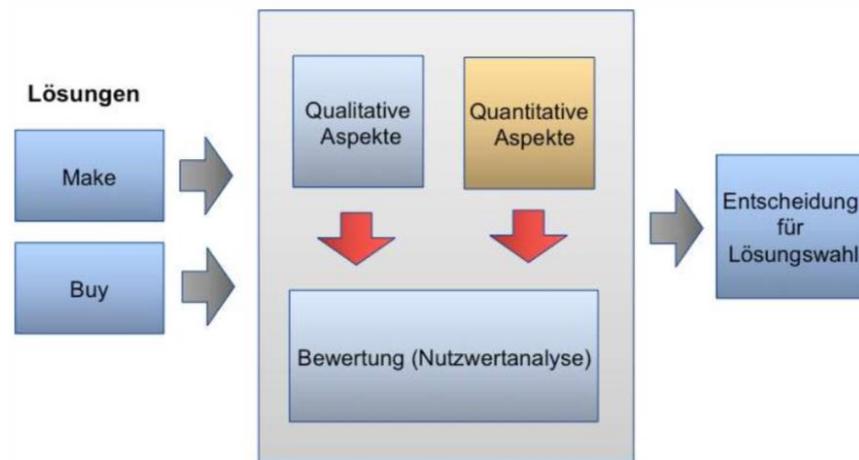
###### **5. Kostensenkung durch Outsourcing?**

Erfahrungsgemäß können die IT-Betriebskosten durch IT-Outsourcing zwischen 15% und 40% reduziert werden.



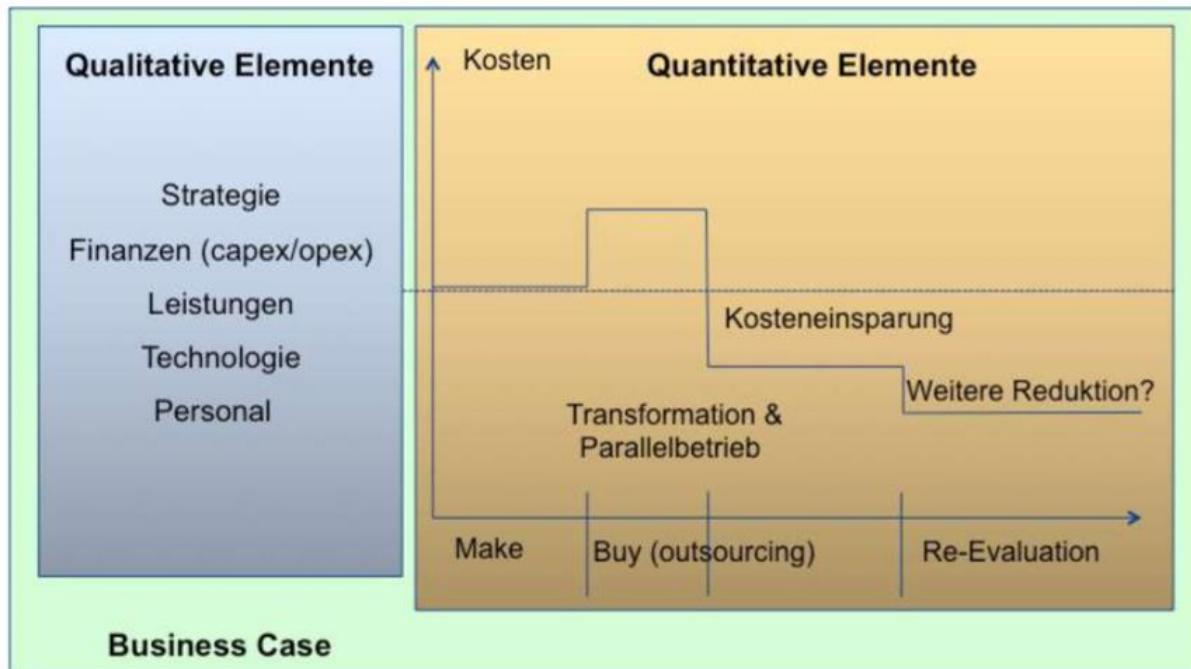
##### 4.5.2 Lösungsbewertung

###### **5. Lösungsbewertung**

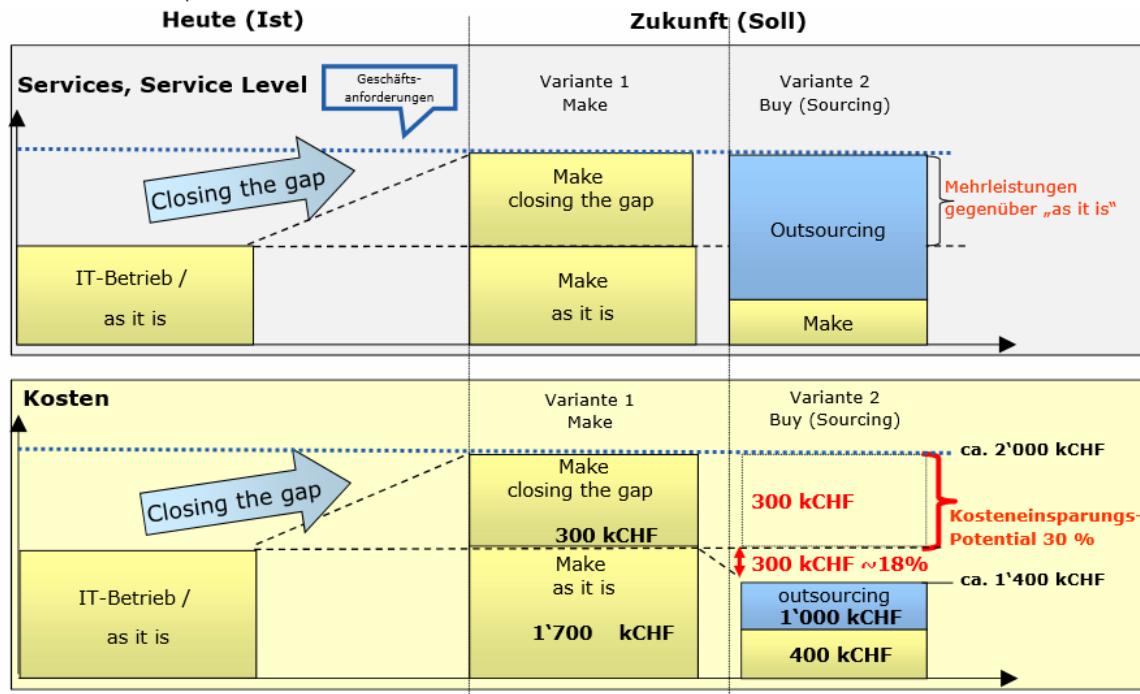


#### 4.5.3 Nutzen im Outsourcing

## 5. Qualitativer & Quantitativer Nutzen im Outsourcing



#### 4.5.4 Praxisbeispiel

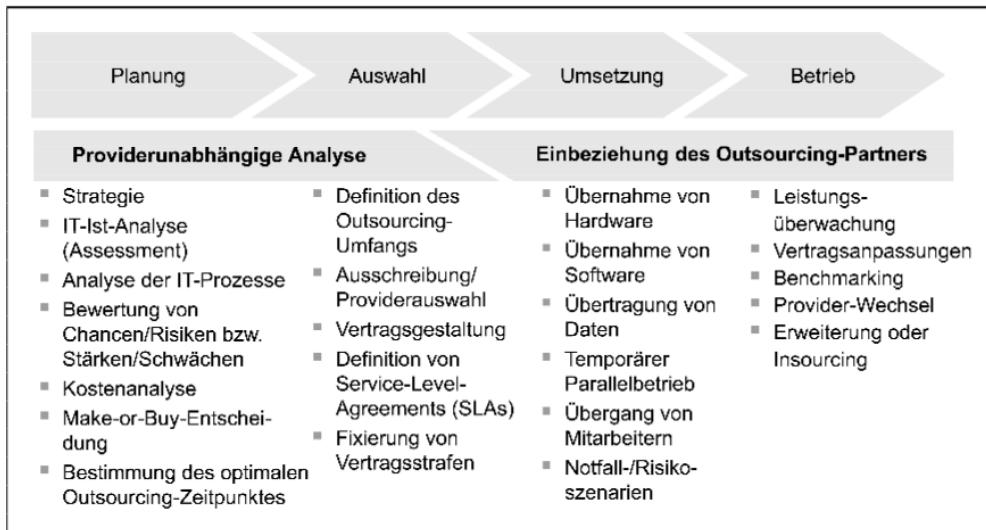


## 4.6 Erfolgsfaktoren vom Sourcing



## 4.7 Outsourcing-Prozess

### Outsourcing-Prozess



## 4.8 SLA

### Service-Level-Agreements (SLA)

- Unter **Service-Level-Agreements (SLA)** versteht man kennzahlenbasierte Vereinbarungen eines Dienstleistungsanbieters mit seinen Kunden bezüglich der zu gewährleistenden Servicequalität.
- Ein **Service Level (SL)** bezieht sich immer auf ein Leistungsmerkmal einer IT-Dienstleistung, z. B. die durchschnittliche Verfügbarkeit eines Systems.
- Die **Leistungsspezifikation** durch die Definition des SL führt dazu, dass die Transparenz erbrachter IT-Leistungen erhöht wird.
- Die für die Einhaltung eines SL relevante Größe bezeichnet man als **Messgröße**. Häufig verwendet werden hier Verfügbarkeitsquoten, Antwort- und Reaktionszeiten, Bearbeitungszeiten, der Personalaufwand zur Erbringung einer Leistung oder die Anzahl der Ausfälle pro Zeiteinheit

#### 4.8.1 Beispiel SLA

### Beispiel: Ergebnisbezogene Service-Levels

Service-Level	Erläuterung
<b>1. Ergebnisbezogene Service-Levels</b>	
Verfügbarkeit	Leistungsbereitschaft eines IT-Systems als Anteil eines Zeitraums (z.B. 98 Prozent/Monat)
Antwortzeit	Ausführungszeit für Benutzertransaktionen (z.B. durchschnittlich 1 sec im Tagesmittel oder 98 Prozent der Transaktionen < 1,5 sec)
Problem-lösungszeit	Maximale Zeit bis zur Lösung eines Problemfalls (in der Regel werden Probleme nach Schwere klassifiziert und danach abgestufte Zeiten vereinbart) (z.B. Behebung eines Störfalls der Stufe 1 (Totalausfall des Systems) innerhalb von vier Stunden)
Zuverlässigkeit	Inhaltung von Zusagen und Arbeitsqualität (z.B. Anteil kritischer Wartungsmaßnahmen, die zum zugesagten Zeitpunkt bereitgestellt werden, oder Anwendungen, die fehlerfrei in den Produktionsbetrieb übernommen werden)
Kunden-zufriedenheit	Zu erreichender Indexwert einer Kundenzufriedenheitsbefragung

#### 4.9 Chancen und Risiken IT-Outsourcing

### Chancen und Risiken des IT-Outsourcing

IT-Outsourcing: Chancen	IT-Outsourcing: Risiken
<ul style="list-style-type: none"> <li>□ Kostensenkung / Fixkostenabbau</li> <li>□ Planbarkeit der Kosten</li> <li>□ bedarfsgerechte Anpassung</li> <li>□ Erhöhung der Flexibilität</li> <li>□ Vermeidung von IT Investitionen</li> <li>□ Abwälzung von Risiken</li> <li>□ erhöhte Innovationsfähigkeit</li> <li>□ professionelle Leistungserbringung</li> <li>□ Zugang zu speziellem Know-how</li> <li>□ Zugang zu modernen Technologien</li> <li>□ Zugang zu Best Practices</li> <li>□ Konzentration auf das Kerngeschäft</li> <li>□ Entlastung von Routineaufgaben</li> <li>□ reduzierte Mitarbeiterabhängigkeit</li> <li>□ Zuführung liquider Mittel (Übergang der IT-Assets)</li> </ul>	<ul style="list-style-type: none"> <li>□ hohe Abhängigkeit vom Dienstleister</li> <li>□ Verzicht auf eigene IT-Kompetenz</li> <li>□ Einschränkung strategischer Optionen</li> <li>□ hohe Umstellungskosten</li> <li>□ Aufwand bei unvorhergesehenen Anforderungen</li> <li>□ Erhöhter Kommunikations-/ Koordinationsaufwand</li> <li>□ Schlechtere Verständigung zwischen IT und Fachabteilung</li> <li>□ Intransparenz der Preise</li> <li>□ langfristige Wirkung</li> <li>□ Irreversibilität der Entscheidung</li> <li>□ Demotivation der Mitarbeiter</li> <li>□ Verlust von Schlüsselpersonen</li> <li>□ Unvereinbarkeit der Unternehmenskulturen</li> </ul>

## 5 Lizenzmanagement

### 5.1 Definitionen

- Das **Lizenzmanagement** beschreibt Prozesse für den legalen Umgang mit Software und deren vereinbarten Lizenz- und Nutzungsbestimmungen.
- Das Lizenzmanagement hat primär eine **wirtschaftliche Sichtweise**.
- Für die gleichzeitig notwendige technische Verwaltung und Steuerung der einzusetzenden Software in einem Unternehmen wird der Begriff **Software-Asset-Management (SAM)** verwendet.
- Der Begriff **Software-Lizenz** bezeichnet das Nutzungsrecht, das der Rechteinhaber (Urheber) dem Nutzer (Endanwender) an der von ihm erworbenen Software einräumt.
- In einem **Lizenzvertrag** wird der vom Urheber vorgegebene rechtliche und vertragliche Rahmen beschrieben. Erst mit dem Akzeptieren des Lizenzvertrags darf die Software in der vereinbarten Form bestimmungsgemäß genutzt werden.
- Das **Verwalten von Software-Lizenzen** bedeutet also:
- *Die rechtskonforme sowie betriebswirtschaftlich optimierte Nutzung von Software-Lizenzen sicherzustellen, diesen Prozess permanent zu überwachen und zu steuern.*

### 5.2 4 Stufen der Einführung

#### Stufe 1: Die Erzeugung verlässlicher Daten

beinhaltet das Wissen über die exakte Anzahl der im Unternehmen eingesetzten Software und der vorhandenen Lizenzen (Nutzungsrechte) sowie die Erstellung von regelmässigen Lizenzbilanzen (Compliance Report).

#### Stufe 2: Die Kontrolle des Umfelds

beinhaltet die Definition und Abbildung von standardisierten Prozessen und Verfahren im Software-Life-Cycle-Prozess, um die erhobenen Informationen stets auf einem aktuellen Stand halten zu können.

#### Stufe 3: Die Einbindung in die Geschäftsprozesse

beinhaltet die Schaffung eines SPOC (Single Point of Contact) für alle Belange des Lizenzmanagements, sowohl organisatorisch, administrativ, technisch als auch lizenziertlich betrachtet.

#### Stufe 4: Die vollständige Integration

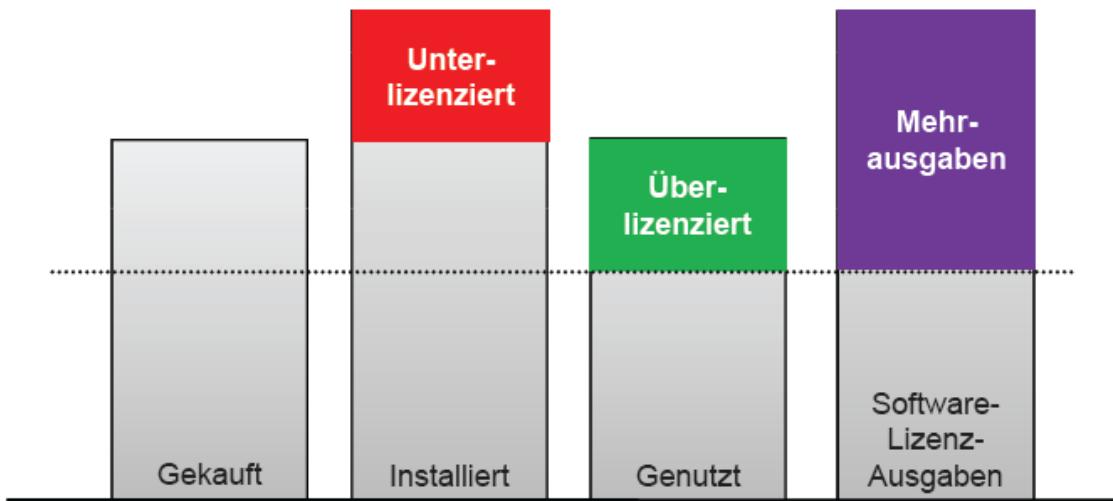
beinhaltet die Umsetzung eines dauerhaften operativen Software-Asset- und Lizenzmanagements mit den erforderlichen eingeführten Prozessen, Rollen und Richtlinien und die dafür notwendige Unterstützung durch ein geeignetes Tool.

#### TIPP

- Nehmen Sie sich erst eine bestimmte Gruppe von Herstellern oder Produkten vor und erstellen Sie daraus eine Top-5- oder Top-10-Liste. Die Auswahl können Sie über die Installationszahlen der Software, strategische Hersteller oder Investitionsvolumen eingrenzen.
- Eine pragmatische und schnelle Variante ist neben einer Sammelrufnummer auch die Einrichtung eines Gruppenpostfachs. Legen Sie fest, dass zukünftig sämtliche Anfragen zu

Software und Lizenzen nur noch an dieses Postfach zu richten sind. Damit haben Sie Ihrem Lizenzmanagement-Team bereits eine wichtige Brücke gebaut, um die anfallenden Aufgaben leichter erfüllen zu können.

### 5.3 Typische Unternehmenssituationen



#### TIPP

- Das Beispiel eines namhaften Herstellers zeigt das ganze Dilemma: Er bietet seinen Kunden rund 3'000 unterschiedliche Softwareprodukte mit 40 verschiedenen Lizenzmodellen an. Allein im Jahr 2010 veröffentlichte er 1'400 Lizenzbestimmungen. Das sind 26 veränderte Bestimmungen pro Woche. Damit steht er keineswegs allein. Alle Anbieter pflegen eine Programmvielfalt mit entsprechend vielen Lizenzmodellen.
- Dank einer effektiveren Verwaltung und Organisation Ihrer Software-Landschaft können Sie diesen Herausforderungen gelassen begegnen. Dafür ist es jedoch notwendig, Spezialwissen über die Software-Lieferanten und deren Lizenzmodelle im Unternehmen aufzubauen.
- Dieses Wissen müssen Sie für den Aufbau und die Organisation des Lizenzmanagements nutzen. Dabei geht es auch darum, Rollen und Zuständigkeiten zu definieren und die damit verbundenen Prozesse abteilungsübergreifend im Unternehmen zu verankern.

### 5.4 Fragen für die erste Bestandsaufnahme

- Können Sie auf Knopfdruck Ihren aktuellen Bestand an PCs, Servern und anderem IT-Equipment abrufen?
- Können Sie ermitteln, wie viele unterschiedliche Software-Anwendungen Sie haben, und werden diese auch alle eingesetzt und tatsächlich genutzt?
- Wird Ihre Software zentral oder dezentral beschafft?
- Werden die Vertragsunterlagen an einer Stelle geführt?
- Was passiert mit der Software, die nicht mehr genutzt wird? Wird das in den bestehenden Verträgen mit betrachtet?
- Kann Software von Mitarbeitern unerlaubt installiert werden?
- Besitzen Sie Richtlinien für den Umgang mit Software in Ihrem Unternehmen?

- Werden diese Richtlinien von jedem verstanden, „gelebt“ und ihre Einhaltung regelmässig überprüft?

#### **TIPP**

In vielen Fällen ist der endgültige Auslöser, ein Lizenz-Managementprojekt zu starten, der angekündigte Besuch eines Auditors, der im Auftrag eines Softwareherstellers bei Ihnen vorstellig wird. Nur ist es dann meistens schon zu spät. Jetzt kostet es Sie unter Umständen richtig viel Geld, da Sie den „Schätzungen“ des Auditors keine eigenen belastbaren Zahlen entgegenhalten können. Zeigen Sie deshalb die Brisanz des Themas bei Ihrer Geschäftsleitung bzw. bei Ihrer Revision noch einmal eindringlich auf, um künftig bei anstehenden Audits besser gewappnet zu sein.

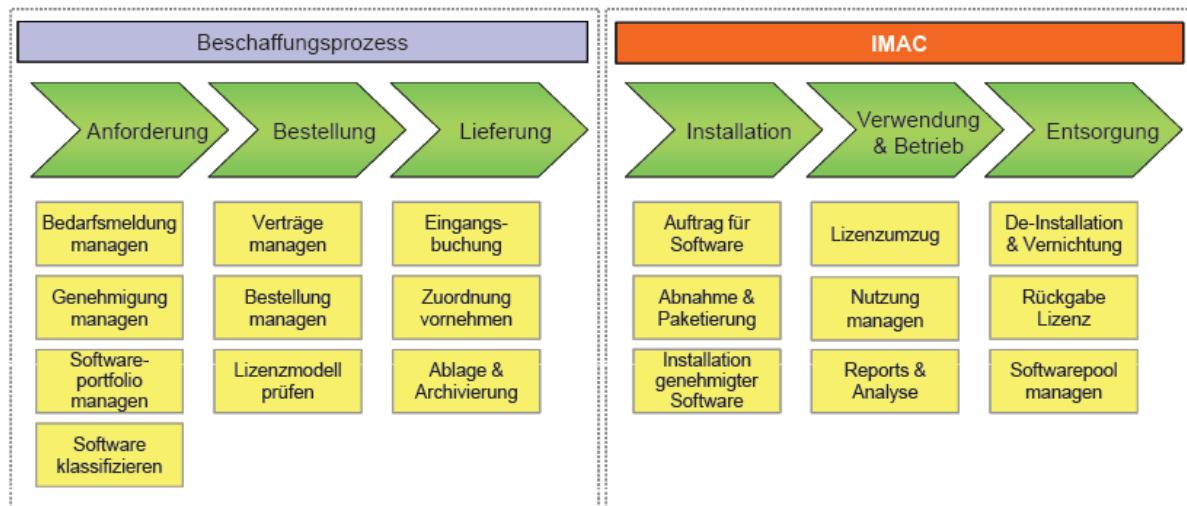
### **5.5 Weitere Vorteilung der Implementierung eines Lizenzmanagements**

- Die Einhaltung der Volumenverträge, z. B. Software License Agreements (SLA)
- Die Beachtung von Vorgaben zur transparenten Darstellung der Unternehmenssituation (Revision)
- Die Schaffung von Compliance (durch den Abgleich der erfassten technischen und kaufmännischen Daten)
- Die Informationsbereitstellung für eine strategische Planung von Software-Einkäufen
- Aufzeigen möglicher Einsparungen durch Steuerung der Lizenzausnutzung
- Einsparungspotenziale durch Wiederverwendung ungenutzter bzw. freier Lizenzen innerhalb eines „Lizenzpools“
- Prozesskostensenkung durch Optimierung des Lizenz- und Software-Handlings (z. B. interner Lizenzbestellvorgang, Lizenzverwaltung)
- Bessere Position gegenüber den Software-Herstellern bei Vertrags-verhandlungen durch eine transparente und aktuelle Sicht der Lizenzierungssituation.

### **5.6 Lizenzmodell**

- **Lizenzmodelle beeinflussen die rechtmässige Software-Nutzung in Form folgender Faktoren:**
  - durch die **Lizenzart** (z. B. Einzellizenz, Mehrplatzlizenz)
  - durch die **Lizenzklasse** (z. B. Vollversion)
  - durch den **Lizenztyp** (z. B. pro Gerät, pro gedruckte Seite)
  - durch die **Lizenzmetrik**, mit der man festlegt, wie gezählt wird (z. B. gilt die Lizenz für 5'000 gedruckte Seiten pro Monat oder für 1'000 zu verwaltende Systeme)

## 5.7 Haupt- und Teilprozesse im Software-Life-Cycle-Prozess



### TIPP

- Wenn Sie planen, ein Lizenzmanagement-Tool einzusetzen und sich davon eine wirkungsvolle Unterstützung erhoffen, müssen Sie im Vorfeld die bestehenden Software-Life-Cycle-Prozesse einer Ist-Analyse unterziehen, um mögliches Optimierungspotenzial aufzeigen zu können.
- In einem zweiten Schritt sollte dann der Software-Life-Cycle-Prozess mit den heutigen Anforderungen im Unternehmen auf den Prüfstand gestellt werden. Denn das Lizenzmanagement-Tool sollte zu den Prozessen des Unternehmens passen und nicht das Unternehmen zu den (eventuell sehr starren) Prozessabläufen des Tools.

## 5.8 Der Lizenzmanager

- steuert und überwacht die Lizenzbeschaffung für alle Objekttypen (Client, Server, Host)
- unterstützt die Fachabteilungen bei der strategischen Software-Bedarfsplanung
- formuliert Richtlinien, Massnahmen und Kontrollmechanismen für den Umgang mit Lizenzen und agiert gemäss den Lizenzmodellen (z. B. Vermeidung von Peaks zum Stichtag der Lizenzzählung)
- begleitet Software-Audits (intern sowie extern) und stellt die hierfür benötigten Auskünfte und Bestandslisten bereit
- verantwortet die Berichtserstellung zum Lizenzierungsstatus für das Management
- plant und initiiert Massnahmen zur Verbesserung der Lizenzmanagement-Prozesse
- kontrolliert die nachhaltige Umsetzung des kontinuierlichen Verbesserungsprozesses aus den erforderlichen Lizenzmanagement-Massnahmen

## 5.9 Fragen zur Erfassung der Lizenz- und Nutzungsdaten

- Wie viele Verträge existieren jeweils von einem Lieferanten zu einem Produkt – pro Unternehmensstandort oder auch übergreifend?
- Sind alle abgeschlossenen Verträge in einem zentralen Einkaufs- oder Vertragsmanagementsystem erfasst?
- Existieren Software-Verträge und Einkaufsabschlüsse möglicherweise nur in Papierform?

- Muss deshalb Schrankware in erheblichem Umfang nacherfasst werden?
- Wie soll die Nacherfassung abgewickelt werden und durch wen?
- Welcher Stichtag wäre für die Erstellung des Lizenzinventars festzulegen?

## 5.10 Zusammenfassung

Das Lizenzmanagement ist für Unternehmen ein Steuerungsinstrument, um „Software“ wirtschaftlich und gemäss den vereinbarten Nutzungsbedingungen der Hersteller einzusetzen. Ein Lizenzmanagement zu entwickeln, aufzubauen und zu implementieren, ist eine grosse Herausforderung.

Der Einsatz eines Werkzeugs ist dabei nur eine Möglichkeit, diesen Prozess zu unterstützen. Viel wichtiger sind die vielen unterschiedlichen Faktoren, die es zu beachten gilt, wenn ein Lizenzmanagement aktiv betrieben werden soll. Beispielsweise spielen das genaue Wissen und die Beachtung der bestehenden IT-Architektur eine grosse Rolle, damit die vereinbarten Nutzungsrechte lizenzkonform umgesetzt werden können. Ebenfalls muss die Managementebene in das Thema Lizenzmanagement eingebunden werden. Denn nur mit der Unterstützung des Managements kann der Lizenzmanager seine Rolle unternehmensweit ausüben. So kann er die Einhaltung der gesetzlichen Vorgaben sowie die ordnungsgemässe Verwendung der durch die Software-Hersteller eingeräumten Nutzungsrechte sicherstellen.

Denn letztendlich geht es darum, eine optimale, den funktionalen und wirtschaftlichen Verhältnissen angepasste Lösung zu finden.

## 6 Musterlösungen von Guido Kaufmann

Seite 1/6

### MUSTERLÖSUNG

Lucerne University of  
Applied Sciences and Arts

**HOCHSCHULE  
LUZERN**

Informatik

#### Repetition und Prüfungsfragen IMR06 IT-Audit Bachelor WI FS-2017

Dozent: Guido Kaufmann

[guido.kaufmann@bluewin.ch](mailto:guido.kaufmann@bluewin.ch)

##### Aufgabe 1: IT-Wertbeitrag

- a) In vielen Unternehmen ist die IT ein «Sorgenkind» des Managements. Was sind mögliche Gründe dafür und wie könnte dem begegnet werden?

- 1)  stetig steigende Kosten  
 wenig Beeinflussbarkeit der Ausgestaltung / Kosten  
 wahrgenommener Wettbewerbsnachteil wegen Langsamkeit

2

- 2)  Transparenz Kosten / Nutzen  
 aufzeigen von Hebeln zum Beeinflussen der Kosten /  
 des Bezugs  
 strukturierter Management des IT-Portfolios

2

- b) Zeigen Sie eine Methode auf, wie Sie den Wertbeitrag einer IT in einem Unternehmen dem Management verständlich machen können. Konkretisieren Sie das am Beispiel eines Krankenversicherers.

- 1) IT-Kosten reduzieren und Profitabilität erhöhen  
Bsp.: Einsatz von Standard-SW/Branchenlösungen
- 2) Operative Unternehmenskosten reduzieren  
Bsp.: Automatisierte Abrechnungssupport durch IT
- 3) Neue Geschäftsideen ermöglichen für Umsatzsteigerung  
Bsp.: Differenziertere Prämien durch Sport-/ Bewegungsnachweis (Schrittzähler)

2

2

2

### Aufgabe 2: Digitalisierung

- a) Nennen Sie je ein konkretes Beispiel wie die Digitalisierung in der Reisebranche anhand der vier Ansatzpunkte Einzug gehalten hat. Denken Sie sich dabei an traditionelle Reiseveranstalter wie Hotelplan, aber auch neue Marktplayer wie AirBnB.

Interne Prozesse:

- automatisierte Verbuchung von bezogenen Leistungen beim Leistungsempfänger (Hotel, Airline,..) 1 statt manuelle Erfassung oder Lohnversand

Services:

- selbständige Stornierungen / Umbuchungen eines Bezugs durch den Kunden 1

Produkte:

- Ausflüge, Ticketsvorbezug oder -reservierung bei Städtereisen im Vorfeld via Internet tätigen 1

Neue Geschäftsmodelle:

- Privatpersonen können ihre Ferienwohnungen selber über eine Plattform anbieten 1

- b) Welches sind die bedeutenden, neuen technologische Entwicklungen/Trends, welche ganz neues Potential erschliessen und so die vierte industrielle Revolution (Digitalisierung) vorantreiben.

- Mobile / Smartphones
- Cloud
- Big Data
- Everything as a Service
- Internet of Things

3

Aufgabe 3: Wirtschaftlichkeit

- a) Welches sind die beiden Anwendungsfelder für Business-Cases?

Investitionsentscheid: "Lohnt es sich Mittel einzusetzen"

2

Variantenauswahl : Welche Variante ist aus wirtschaftliche / strategische Sicht die beste

1

- b) Welche Aspekte sollte ein Business-Case mindestens abdecken?

- Strategie oder Risiko/Handlungsbedarf
- Varianten (auch Variante nichts tun)
- Kosten / Nutzen → Wirtschaftlichkeit

3

c) Was sagt der NPV in einem Business-Case aus?

Wert der Investition über Beobachtungsraum  
(unter Berücksichtigung der Diskontierung)

2

d) Was beabsichtigte die IT-Leitung der Hotelplan-Gruppe mit der Einführung des ValIT-Frameworks?

stärker den Nutzen der IT-Investitionen  
ausweisen und verfolgen (IT-Wertbeitrag)

2

gezieltere Steuerung der IT-Investitionen  
nach Nutzen (Portfolio-Management)

2

und Strategiekonformität

#### Aufgabe 4: Outsourcing

- a) Outsourcing wird häufig mit einer Kosteneinsparung in Verbindung gebracht. Wo bietet sich Potential, zum Beispiel beim Outsourcen der ganzen Workplace-Infrastruktur (PCs incl. Servicedesk) (siehe Folie 26)

- 1) IT-Umgebung des Dienstleisters: Konsolidierung und Standardisierung (geteilte Engineering & Businessprozesse z.B. für IMAC, Fieldforce, ...)
- 2) Nutzung weltweiter Kapazität: Off-/Nearsharing (z.B. Servicedesk in Polen)
- 3) Operational Excellence: PC-Betrieb gleich Kerngeschäft des Outsourcers (z.B. früh Erfahrung mit Cloud-Services)

- b) Nennen Sie drei Erfolgsfaktoren bei einem Outsourcing und erläutern Sie diese kurz hinsichtlich Risiken.

Begriff Erfolgsfaktor = Elemente die für erfolgreiches Vorhaben wichtig sind

- 1) Strategie : Outsourcing = langfristiges Vorhaben, zickzack-fahren wird teuer
- 2) Governance : klares Arbeitmodell, sonst Doppelpunktreihen oder Lücken, die teuer werden
- 3) Ausschreibungsunterlagen: Damit im Betrieb dann nicht Diskussionen u. Zusatzkosten entstehen
- 4) Vertrag : Wenn Unstimmigkeiten oder gar Streitereien entstehen, reduziert ein guter Vertrag rechtliche, finanzielle Risiken
- 5) Beziehungsmanagement: Immer an der Beziehung arbeiten um ggf. nie in rechtl. Diskussionen zu kommen

**Aufgabe 5: Lizenzmanagement**

- a) Beschreiben Sie die Hauptprozesse im Software-Life-Cycle-Prozess!

Beschaffungsprozess

Anforderung - Bestellung - Lieferung

2

ILAC (Installation, Umzug, ...)

Installation - Verwendung / Betrieb - Entsorgung

2

- b) Begründen Sie 2 Vorteile, die für die Einführung eines IT-Lizenzmanagements sprechen!

Bessere Wirtschaftlichkeit durch Vermeidung von Falsch- / Überlizenzen / höhere Verhandlungsmacht

2

Compliance, d.h. keine rechtlichen Probleme

2

## 7 IT Audit-Planung

### Audit (FS):

Ziel einer Abschlussprüfung ist die Abgabe eines Urteils darüber, ob der Abschluss in allen wesentlichen Punkten den anzuwendenden Rechnungslegungsnormen entspricht

(Die Abschlussprüfung soll die Abgabe eines Urteils darüber ermöglichen, ob der Abschluss wesentliche Fehlaussagen enthält.) (PS 200)

### Abgrenzungen:

- **Interner (IT-)Audit:** Langfristige Sicherung der Interessen der Unternehmung und der Eigenkapitalgeber
- **Externer (IT-)Audit:** Beschränkt auf Einfluss auf finanzielles Audit

### 7.1 Rahmenbedingungen

#### Gesetze

- **Obligationenrecht**
  - Art. 728a: Die Revisionsstelle prüft, ob die Jahresrechnung und gegebenenfalls die Konzernrechnung den gesetzlichen Vorschriften entspricht;
  - Art. 957a, Absatz 2: Die Buchführung folgt den Grundsätzen ordnungsmässiger Buchführung. Namentlich sind unter anderem zu beachten: **Belegnachweis** und **Nachprüfbarkeit**
- **Geschäftsbücherverordnung**
  - Art. 1, Absatz 1: Wer buchführungspflichtig ist, muss ein Hauptbuch und... auch Hilfsbücher führen
  - Art. 2, Absatz 2: Werden die Geschäftsbücher elektronisch oder auf vergleichbare Weise geführt und aufbewahrt und die Buchungsbelege sowie die Geschäftskorrespondenz elektronisch oder auf vergleichbare Weise erfasst und aufbewahrt, so sind die Grundsätze der ordnungsgemässen Datenverarbeitung einzuhalten.
  - Art. 2, Absatz 3: Die Ordnungsmässigkeit der Führung und der Aufbewahrung der Bücher richtet sich nach den allgemein anerkannten Regelwerken und Fachempfehlungen...

#### Richtlinien

- **Schweizer Prüfungsstandard**
  - PS 200: Ziele und allgemeine Grundsätze
  - PS 400: Risikobeurteilung und interne Kontrolle
  - PS 401: Prüfung im Umfeld der Informations- und Kommunikationstechnologie

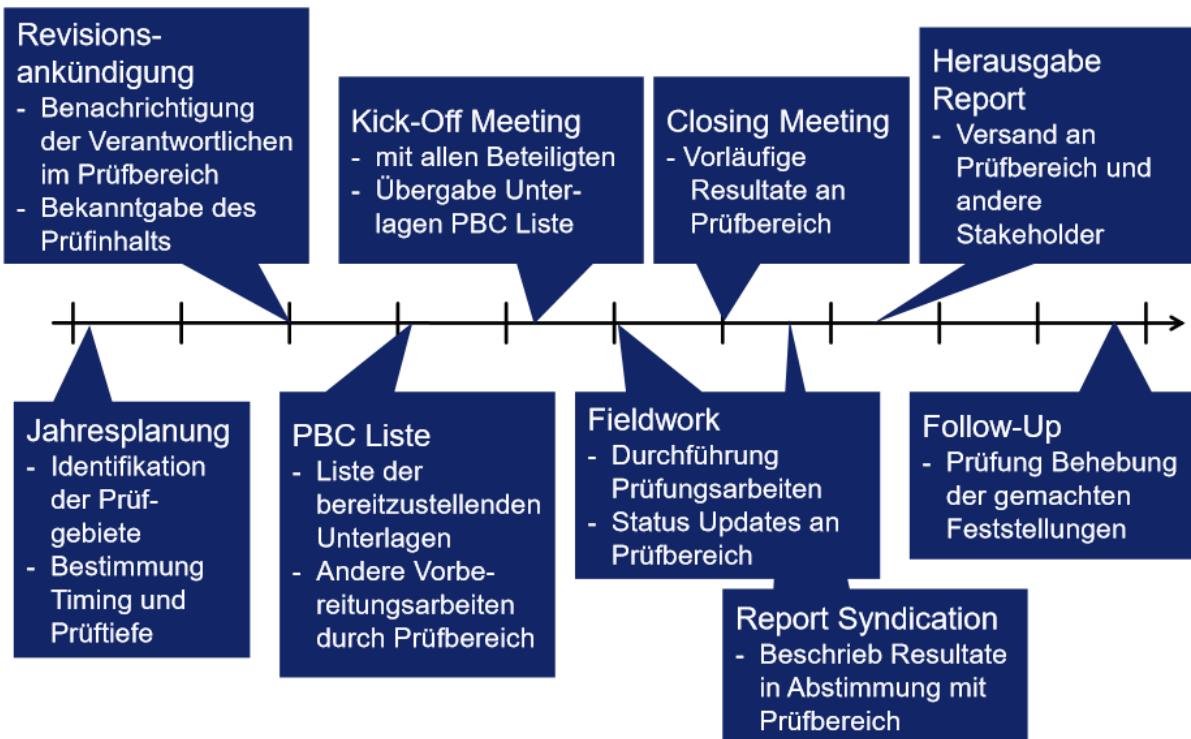
#### Branchenvorschriften

- Handbuch der Wirtschaftsprüfer

### 7.1.1 Ziele Prüfung Finanzberichterstattung

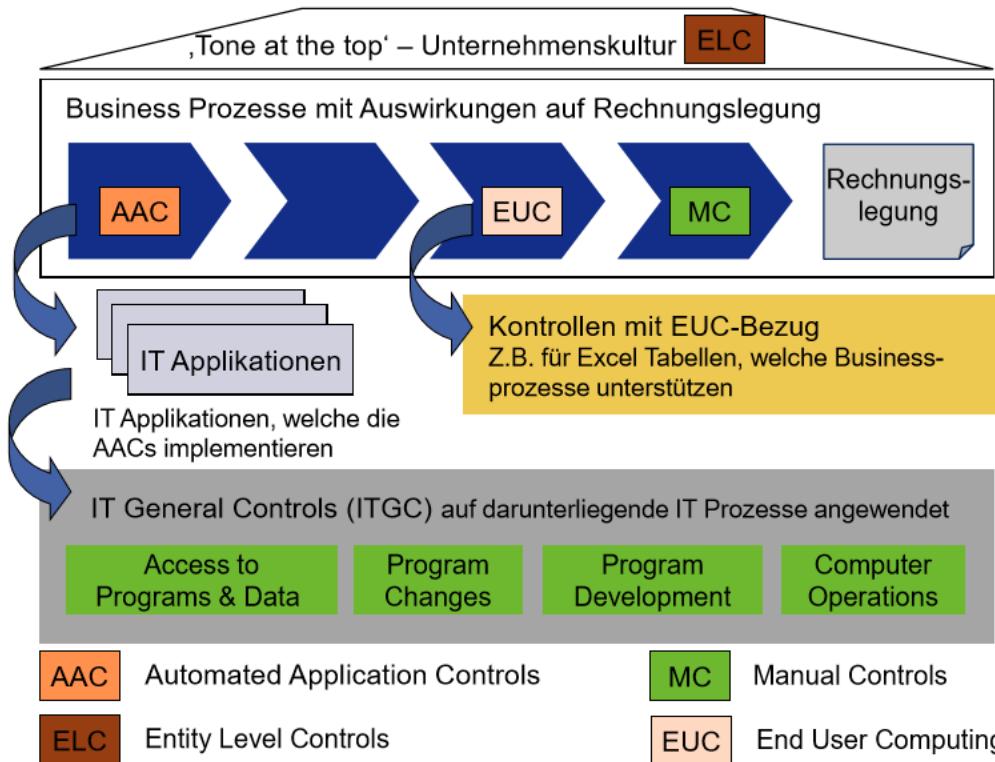


### 7.2 Timeline

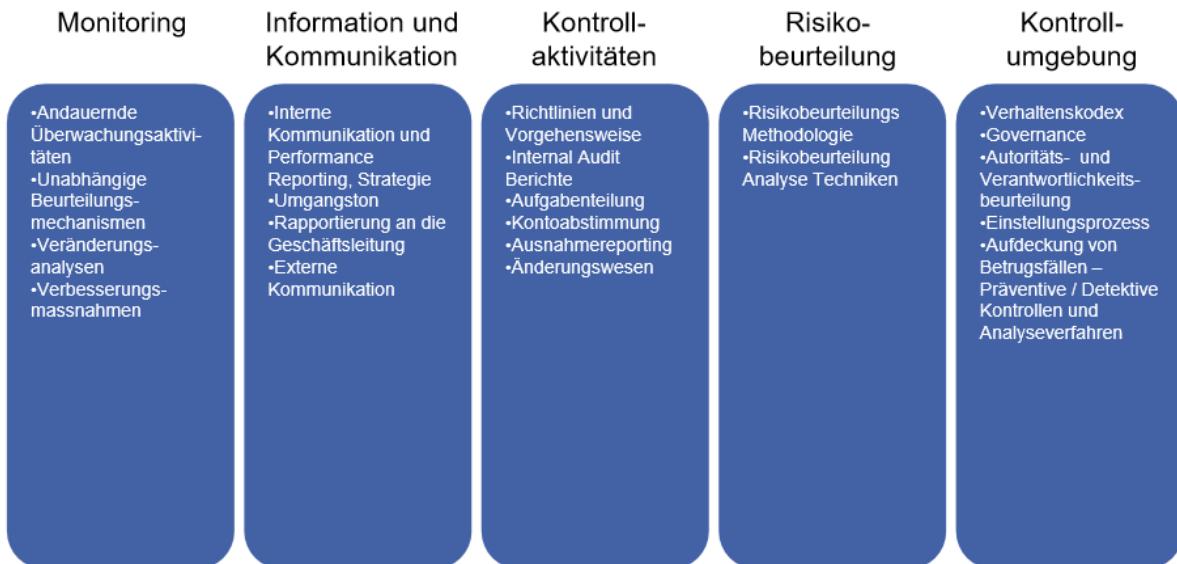


## 8 Prüfungsdurchführung

### 8.1 Kontrollarten



#### 8.1.1 Entity Level Controls



## Prüfung von Entity Level Controls (ELC)

Aufgrund der Eigenschaften von Entity Level Controls besteht eine Prüfung hauptsächlich aus

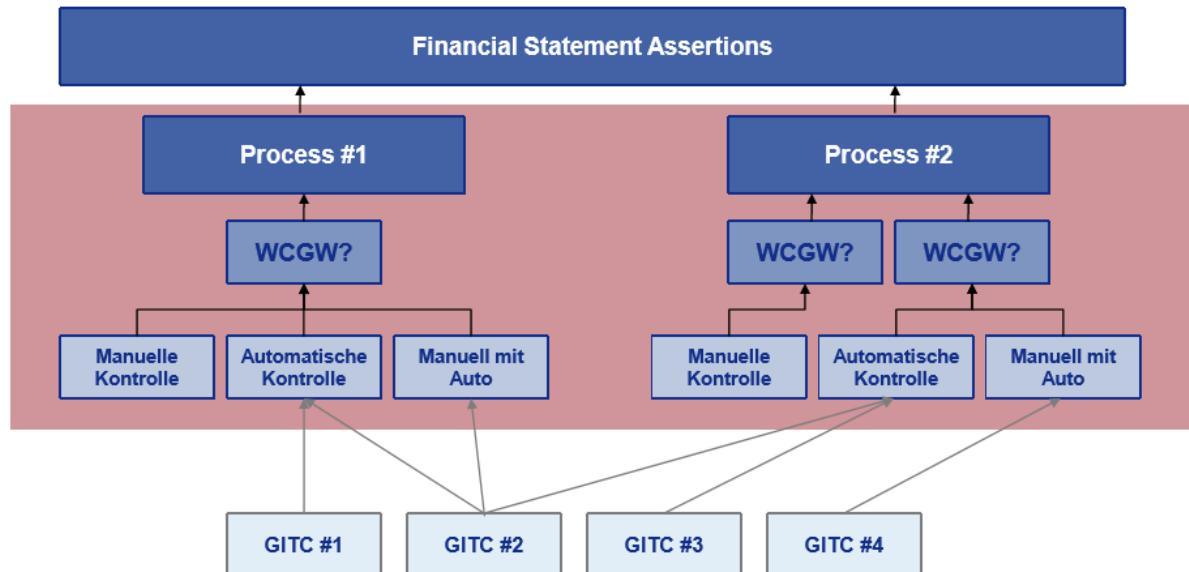
- Interviews mit der Geschäftsleitung / Top Management
- Inspektion von Strategiedokumenten, internen Weisungen und Richtlinien

Ziel ist, angemessene Sicherheit darüber zu erhalten, dass das Unternehmen über ausreichende Kontrollen über die generelle Leistungserbringung und Unternehmenskultur verfügt. Es finden in der Regel keine oder nur beschränkte Operating Effectiveness Tests statt. ELC sind in der Regel manuelle Kontrollen.

Beispiele:

- Prüfung, ob eine IT Strategie existiert, angemessen mit der Business Strategie übereinstimmt, periodisch aktualisiert wird und für die Mitarbeiter im Intranet verfügbar ist.
- Prüfung ob die internal Audit Funktion eines Unternehmens angemessen von der übrigen IT Leistungserbringung getrennt ist und direkt dem Audit Committee des Verwaltungsrates rapportiert.

### 8.1.2 Process Level Controls



## Typische automatisierte Process Level Controls:

Eingabekontrollen	Beispiel
▪ Input Autorisierung	Signierte Inputform, autorisierter User
▪ Batch Kontrollen	Summentotal, Anzahl Zeilen, Hash Total
▪ Exception Reporting	Flagging von bestimmten Transaktionen
Verarbeitungskontrollen	
▪ Datenvalidierung	Limiten, Data Range, Doppelinträge
▪ Programmprüfungen	Nachkalkulation
▪ Abstimmungen	Vollständigkeit und Genauigkeit der Daten in zwei Systemen
▪ Exception Reporting	Nachverfolgung von Fehlern
Ausgabekontrollen	
▪ Logging und Archivierung	Logging aller erfolgten Verarbeitungen
▪ Reportverteilung	Markierte Exemplare pro Person, Labelling

## Zusicherungen (Assertions) für automatisierte Process Level Controls (und GITC):

### Vollständigkeit - Completeness

- Sämtliche Relevanten Daten wurden übertragen / verarbeitet

### Genauigkeit - Accuracy

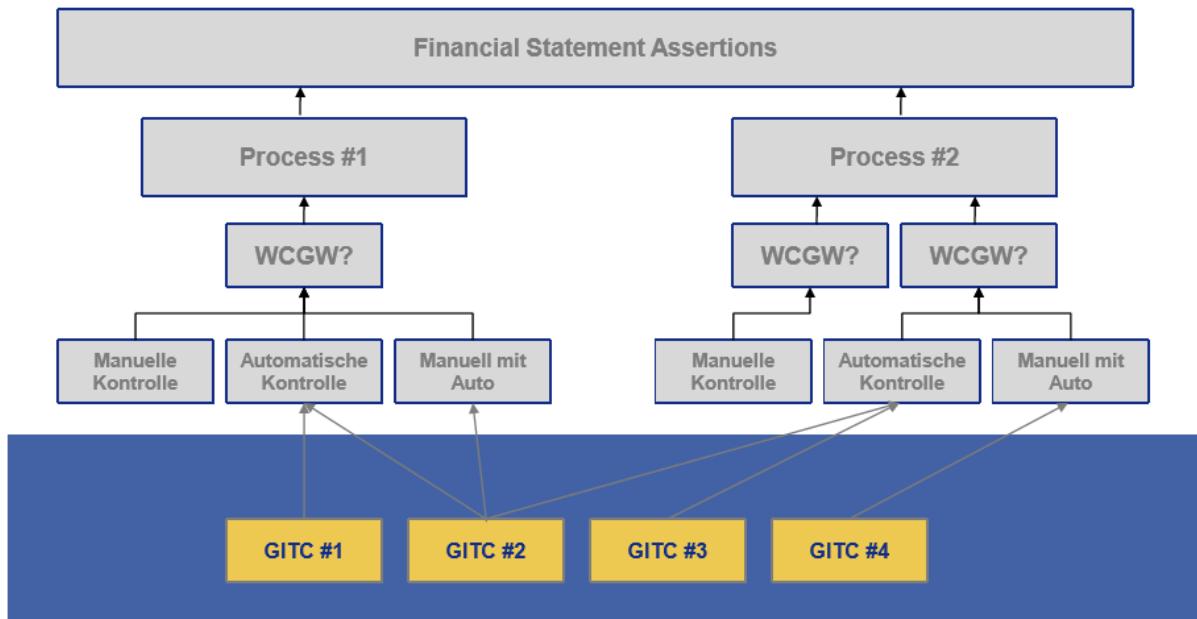
- Daten werden genau so verarbeitet wie sie eingegeben wurden
- Accuracy ist nicht nur bei der eigentlichen Verarbeitung sondern auch bei Schnittstellen wichtig

### Existenz - Existency

- Die geprüften Dinge existieren tatsächlich

Die Wirtschaftsprüfung kennt noch weitere Zusicherungen, Validation, Obligations & Rights und Presentation, welche aber für IT Kontrollen in der Regel keine Anwendung finden

### 8.1.3 General IT Controls



#### Wieso überhaupt General IT Controls?

- Unterstützen das Funktionieren von Process Level Controls über die ganze Prüfperiode hinweg
- Stellen Grundsicherheit für die zu prüfende IT
- Tiefe, in welcher geprüft wird, hängt von den zu unterstützenden Process Level Controls ab

#### Prüfbereiche für General IT Controls:

- Zugriff auf Programme und Daten (inkl. physischem Zutritt)
- Änderungswesen
- IT Entwicklung
- IT Betrieb

Für jeden Bereich existieren generische Kontrollziele, welche in der Regel für die Prüfung herangezogen werden. Die tatsächliche Umsetzung im Unternehmen hängt dann von der jeweiligen IT Umgebung ab.

#### 8.1.4 Assertions

- **Completeness (Vollständigkeit)**
  - There are no unrecorded assets, liabilities, classes of transactions or undisclosed items
- **Existence (Vorhandensein, Existenz)**
  - an asset or liability at a given date and recorded transactions within a class occurred during the period covered by the financial statements
- **Accuracy (Richtigkeit, Korrektheit)**
  - details of assets, liabilities and classes of transactions are correctly recorded, processed and reported with respect to party, allocation to the proper period, description, quantity and price
- **Valuation (Bewertung, Wertung)**
  - assets are recorded at an appropriate amount
- **Obligations and rights (Verpflichtungen und Rechte)**
  - the entity has the appropriate rights (such as title) to the assets reflected in the financial statements. The liabilities reflect the entity's obligations
- **Presentation and disclosure (Einordnung und Ausweis)**
  - an item is disclosed, classified and described in accordance with the applicable financial reporting framework including the application of accounting literature.

**Folgende Prüfprozeduren können ausgeführt werden, um die oben besprochenen Assertions abzudecken:**

Prüfprozedur	Erklärung
Inspection	Betrachtung von Transaktionen, Dokumenten oder physischen Assets
Observation	Beobachtung der tatsächlichen Kontrollausführung
Inquiry	Interviews und Bestätigung des gesagten in zusätzlichen Dokumenten
Computation	Nachrechnen von Kontrollen
Analytical procedures	z.B. Vorjahresvergleich, Plausibilisierung mit Drittinformationen

### 8.1.5 Kontrolleigenschaften

**Prüfungen können entweder verfahrensorientiert oder ergebnisorientiert durchgeführt werden.**

Ergebnisorientierte Prüfungen orientieren sich am Resultat, in der Regel an konkreten Zahlen, während verfahrensorientierte Prüfungen bestätigen, dass ein Prozess robust genug ist, um das Resultat herzustellen.

Bei verfahrensorientierten Prüfungen stehen Kontrollen in Prozessen im Mittelpunkt. Kontrollen können folgende Eigenschaften haben:

- **Wirkung:** detektiv / präventiv
- **Ausführungsart:** manuell / automatisch / halbautomatisch
- **Häufigkeit Ausführung:** jährlich, monatlich, quartalsweise, halbjährlich, bei Bedarf

**Zusätzlich sind auch folgende Risiken bei der Klassifizierung von Kontrollen relevant:**

- Inherent Risk    Inhärentes Risiko des Prozesses, ohne Berücksichtigung der Kontrolle
- Control Risk    Risiko, dass ein materieller Fehler nicht durch die Kontrolle erkannt wird

## 8.2 Manuelle Kontrollen

### Eigenschaften

- Menschliche Komponente → schwieriger einzuschätzendes Kontrollrisiko, abhängig von
  - Kompetenz
  - Objektivität des Kontrolldurchführenden
- Verschiedene Kontrolldurchführende können zu ‚Qualitätsschwankungen‘ führen
- Die operationelle Effektivität muss in der Regel mit Stichproben geprüft werden

Die Prüfung manueller Kontrollen ist deshalb in vielen Fällen aufwändiger als die Prüfung von automatischen Kontrollen

Beachte: Viele Generellen IT Kontrollen sind manuell oder halbautomatisch!

Kontrollbeispiele:

- Jede IT Änderung wird auf einem Papierformular schriftlich vom Business und vom IT Verantwortlichen bewilligt, bevor sie in die Produktionsumgebung eingespielt wird.
- Sämtliche Benutzerrechte werden jährlich durch den Applikationsverantwortlichen einem Review unterzogen. Die notwendigen Änderungen werden dann vom Security Team umgesetzt.

## 8.2.1 Stichprobenprüfung

### Arten von Stichproben

- Statistical Sampling
    - Attribute Sampling
    - Variable Sampling
  - Non-statistical Sampling
- Basierend auf statistischen Methoden
- Vorkommen eines bestimmten Werts
- Wertbasiert, z.B. Schätzung des Werts der Gesamtpopulation
- Basierend auf Erfahrung des Auditors

**Es gibt aber auch Mischformen, z.B.**

- Stratified Sampling
- Statistische Prüfung für bestimmte Transaktionstypen (welche z.B. basierend auf Vorwissen ausgewählt wurden)

### Zu beachten:

- Stichprobengröße hängt von der Gesamtpopulation und vom erwarteten Fehlerwert ab
- In der Praxis werden oft Tabellen verwendet

Frequency of control activity	Minimum sample sizes	
	Risk of Failure	
	Lower	Higher
Annual	1	1
Quarterly	1+1	1+1
Monthly	2	3
Weekly	5	8
Daily	15	25
Multiple times per day	25	40

## 8.3 Automatische Kontrollen

### Eigenschaften

- Kontrollausführung erfolgt automatisiert – Fehlerrisiko ist in der Regel geringer
- Wird die Kontrolle einmal als korrekt geprüft, so funktioniert sie immer gleich,
- SOFERN die sie unterstützenden Generellen IT Kontrollen richtig funktionieren
- UND in der Prüfperiode keine Änderungen an der Kontrolle vorgenommen wurden
- Deshalb kann die Operationelle Effektivität oftmals mittels eines ‚Test of One‘ geprüft werden

Beachte: In der Regel werden keine Generellen IT Kontrollen von automatisierten Generellen IT Kontrollen geprüft

### Beispiele:

- Die Software für den Zahlungsverkehr stellt sicher, dass jede manuell erfasste Zahlung durch einen Teamleiter im Zahlungsverkehr freigegeben werden muss, bevor sie ausgelöst wird. Teamleiter können selbst keine Zahlungen erfassen.
- Das System berechnet monatlich die Kontogebühren aufgrund der vereinbarten Zinssätze und belastet diese jedem einzelnen Kunden.

### 8.3.1 Prüfung

#### Test of One

- Viele automatische Kontrollen können mit einem ‚Test of One‘ geprüft werden
- Dies bedeutet, dass die Kontrolle anhand einer Transaktion durchgespielt oder nachvollzogen wird. Falls diese Transaktion richtig behandelt wird, so können wir davon ausgehen, dass die Kontrolle immer richtig funktioniert.
- ABER: Falls die Kontrolle verschiedene Arten von Transaktionen unterschiedlich behandelt, so muss für jede einzelne Transaktionsart ein separater Test of One durchgeführt werden

Anwendung auf das Beispiel von der vorherigen Folie:

- Wir prüfen eine Berechnung der Kontogebühren anhand der Kontoabrechnung von Herrn Müller, einem Retailkunden. Dabei lassen wir uns den Kontostand aus dem System geben, prüfen die Kontokonditionen von Herr Müller und die Berechnung der Kontogebühren. Dabei stellen wir dann fest, dass die Berechnung für Private Banking und Retail Kunden im System unterschiedlich parametrisiert ist. Zur Sicherheit prüfen wir also analog noch ein Beispiel zu Herrn Huber, einem Private Banking Kunden.

### 8.3.2 Benchmarking

#### Falls eine automatische Kontrolle

- sich seit der letzten Prüfung nicht verändert hat
- die Generellen IT Kontrollen seit der letzten Prüfung durchgehend geprüft wurden und als effektiv beurteilt wurden

kann das letzte Resultat der Prüfung der automatischen Kontrolle als sogenannte Baseline verwendet werden (im Sinne eines **Benchmarking**). In der Regel ist so eine Prüfung nur alle 3 Jahre notwendig.

**ABER: Wie beweise ich, dass die automatische Kontrolle nicht verändert wurde?**

### 8.4 Verhalten bei Exceptions

**Verhalten bei Fällen, wo die Kontrolle für ein Test-Item versagt hat, hängt von Art der Kontrolle sowie den Erwartungen ab:**

- Automatische Kontrolle                          Die Kontrolle ist als nicht effektiv zu beurteilen (einmal falsch, immer falsch)
- Manuelle Kontrolle
  - Keine Abweichungen erwartet                          ev. Testen einer zweiten Stichprobe (grösser oder gleich der ursprünglichen)
  - Abweichungen tolerierbar                                  Anzahl tolerierbare Fehler abhängig von Stichprobe

Sample sizes Risk of Failure		Number of acceptable control deviations
Lower	Higher	
50	80	1
60	95	2
71	111	3
85	133	4
98	154	5
...	...	...

#### 8.4.1 Re-testing:

**Wenn Kontrollschwächen nach unserer Prüfung aber noch in der Prüfperiode behoben werden, müssen wir zur abschliessenden Beurteilung noch einmal einen Test durchführen.**

- Beurteilung der Behebung der Kontrollschwäche
- Behebung per welchem Datum
- Beurteilung des Einflusses der Kontrollschwäche für die Zeit, in welcher sie bestand (abhängig von der Art der Kontrolle!)
- Identifikation von zusätzlichen Kontrollen, welche mitigierend wirken (siehe nächste Folie)
- Bestimmung von zusätzlichen, tiefergehenden Prüfprozeduren, um tatsächliche Auswirkungen der Kontrollschwäche zu bestimmen, z.B.
  - Prüfung der Gesamtpopulation für die Kontrolle
  - im Schlimmsten Fall: Wechsel zu einem ergebnisorientierten Prüfansatz

#### 8.4.2 Kompensierende Kontrollen

Der Einfluss einer Kontrollschwäche auf das zu Prüfende Kontrollziel kann durch mitigierend wirkende Kontrollen ganz oder teilweise aufgehoben werden

Durch die Identifikation und Prüfung von mitigierend wirkenden Kontrollen können also die Auswirkungen auf unser Prüfverfahren bzw. das Prüfresultat verringert werden

#### **Beispiel**

Bei der Prüfung des Benutzeradministrationsprozesses haben wir festgestellt, Applikationsberechtigungen nicht durchgehend entfernt wurden, wenn ein Benutzer das Unternehmen verliess.

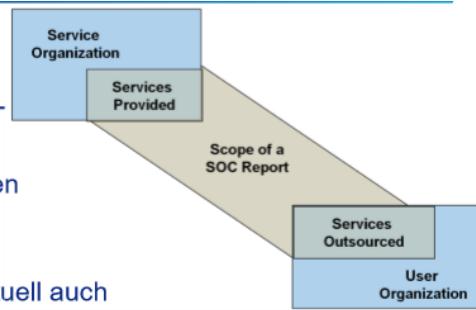
Mitigierend wirken folgende Kontrollen:

- Es findet quartalsweise eine Überprüfung sämtlicher Applikationsberechtigungen durch die Teamleiter statt. Diese müssen bestätigen, dass sämtliche Benutzer ihre Rechte im System tatsächlich benötigen. ABER: Dies lässt potentiell immer noch 90 Tage offen.
- Bei Terminierung eines Mitarbeiters wird ihm umgehend der Windows-Login deaktiviert

## 8.5 Attestation Reports

### Hintergrund / Problemstellung

- Immer mehr Organisationen lagern Teile ihrer Leistungs-erbringung an einen Dienstleister aus
- Nicht nur IT Prozesse, immer mehr Kernprozesse werden ausgelagert. Viele Prozesse sind aus Finanzprüfungs-sicht relevant
- Dies bedeutet, dass wir im Rahmen einer Prüfung eventuell auch Prozesse und Kontrollen bei einem Dienstleister beurteilen müssen



### Lösungsansätze

- Alle Kunden des Dienstleisters schicken ihre Prüfer und diese beurteilen die Kontrollen beim Dienstleister
- Der Dienstleister lässt von (s)einer Prüfgesellschaft einen Bericht zuhanden seiner Kunden erstellen, welcher diesen Sicherheit über die relevanten Kontrollen gibt. Man spricht von sogenannten: **Attestation Reports**

Ein Attestation Report macht entweder nur eine Aussage zum Design der Kontrollen (Type I) oder auch zu ihrer Operativen Effektivität (Type II)

### Der Nutzen eines Attestation Reports für eine Prüfung hängt von folgendem ab:

Relevanz der abgedeckten Kontrollen im Report für unsere Prüfung

- Die Kontrollen müssen genügend Sicherheit über die ausgelagerten Prozesse geben
- Die Kontrollen werden in dieser Form für unser Unternehmen erbracht (der Report wurde für uns erstellt)

Abgedeckte Zeitperiode

- Der Report deckt dieselbe Zeitperiode ab wie wir prüfen
- Allfällige Unterschiede werden durch Bridge Letter abgedeckt, in welchen das Revisionsunternehmen bestätigt, dass sich die Kontrollen seit der Erstellung des Reports nicht verändert haben

Resultat der durchgeföhrten Prüfung

- Die Kontrollen werden als effektiv beurteilt oder anderenfalls im Detail beschrieben, was nicht effektiv war
- Bei ineffektiven Kontrollbereichen stellt sich die Frage, ob mitigierende Kontrollen in unserem Unternehmen existieren, welche das Risiko vermindern

## 8.6 End User Computing

### **Definition End User Computing (EUC):**

Einsatz von IT Mitteln (IT Applikationen) ohne, dass der Einsatz durch Generelle IT Kontrollen einer internen IT Organisation unterstützt wird. Z.B. Applikationsfunktionalität in MS Excel oder Access

### **Risiko:**

Durch fehlende Kontrollen in den Generellen IT Kontrollen kann die Korrektheit und Richtigkeit der Verarbeitung in der EUC selbst nur sehr schwer beurteilt werden.

### **Beispiel:**

Vorfall	Kontrolle
Bei einem Versicherungsunternehmen wurde bei der Verfeinerung der Berechnung zukünftiger Aufwendungen für Überschussbeteiligungen in einem Excel Worksheet eine falsche Position berücksichtigt. Dadurch musste der Reingewinn um über CHF 300 Mio berichtet werden.	Die End User Computing Kontrolle bezüglich der Berechnungen in dem betreffenden Excel Worksheet war nicht vorhanden. Es hatte kein sauberes Testing der Funktionalität stattgefunden.

### 8.6.1 GITC-Kontrollen

#### **Wie können wir dennoch Sicherheit über die Generellen IT Kontrollen einer EUC Applikation erlangen? → Individuelles Testen**

##### **Zugriff auf EUC Applikation**

- Schutz des Ordners, wo die Applikation abgelegt ist
- Zugriffsenschutz der Applikation (z.B. Passwortschutz in Excel)

##### **Änderungswesen**

- Schutz des Programmcodes (z.B. Passwortschutz in Excel)
- Speicherung der Programmversionen in einem Versionierungssystem (z.B. Sharepoint)
- Klares Testing und formelle Abnahme neuer Programmversionen
- Ev. Prüfung, was für Änderungen tatsächlich am Code vorgenommen wurden

##### **Betrieb**

- Periodisches Backup der benutzten Applikation

## 9 IT Audit Frameworks

### 9.1 ISACA

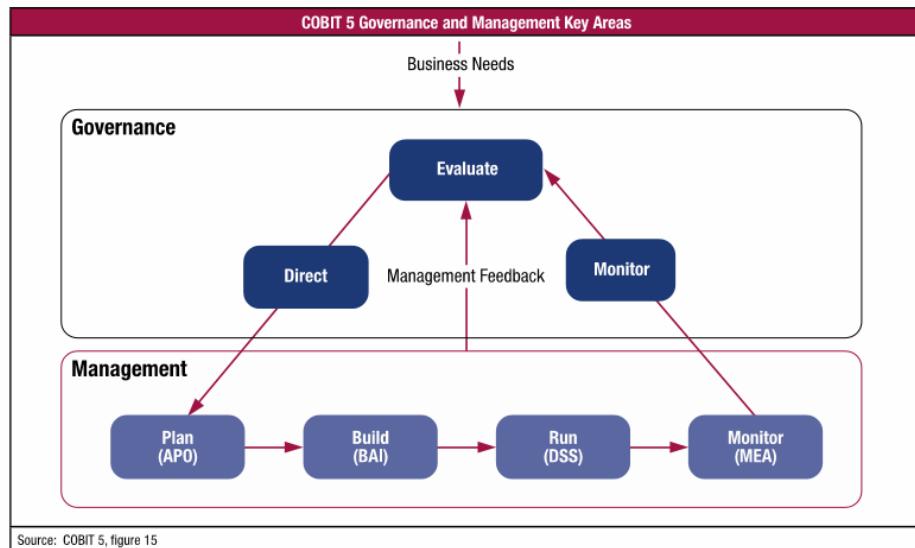
#### Information Systems Audit and Control Association

- **Globale Organisation der IT Revisoren und verwandten Funktionen**
- **Bieten verschiedene Zertifizierungen an**
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified in the Governance of Enterprise IT (CGEIT)
  - Certified in Risk and Information Systems Control (CRISC)
- **Verwaltet verschiedene Hilfsmittel und Standards zur Durchführung von IT Audits**
- **Standards sind für Mitglieder verbindlich**
- **Publiziert COBIT Framework**

### 9.2 Cobit

- **Steht für „Control Objectives for Information and Related Technology“**
- **Entwickelt von ISACA**
- **Umfassendes IT Governance und Management Framework**
- **Kontinuierlich weiterentwickelt von Bottom-Up Ansatz zu heutiger Version, welche auch von den Unternehmenszielen aus Top-Down verwendet werden kann.**
- **Neueste Version 5 wurde im Frühling 2012 publiziert**
- **Beinhaltet in der neuesten Version auch Risk Management und Value Management Komponenten**



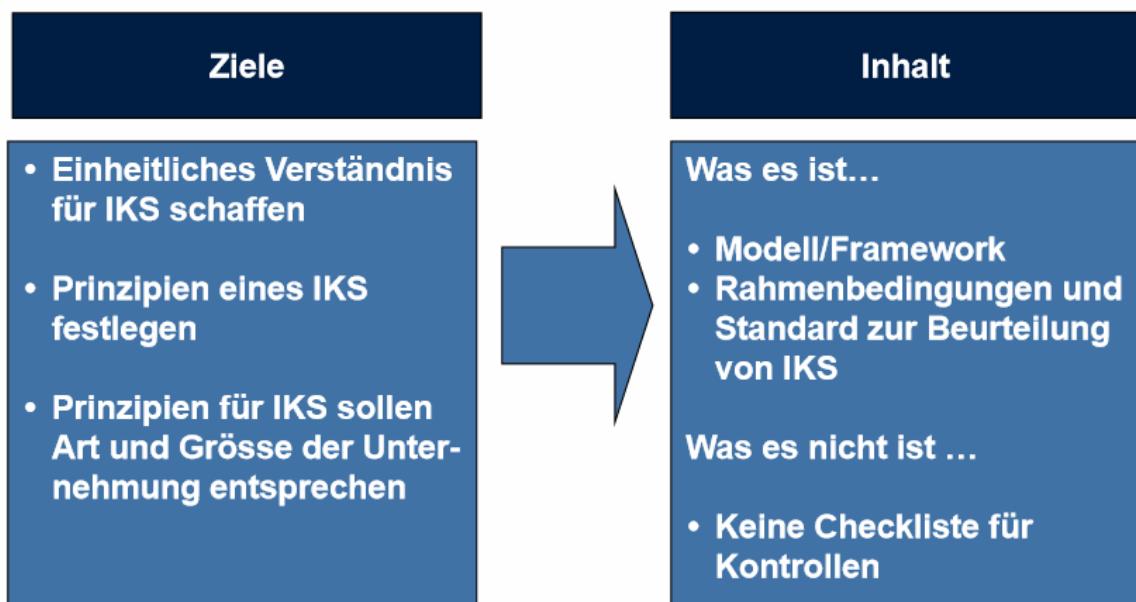


**Governance** ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against plans.

**Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

### 9.3 COSO

#### Best Practice Framework für ein Internes Kontrollsystem (IKS)



### 9.3.1 Dimensionen

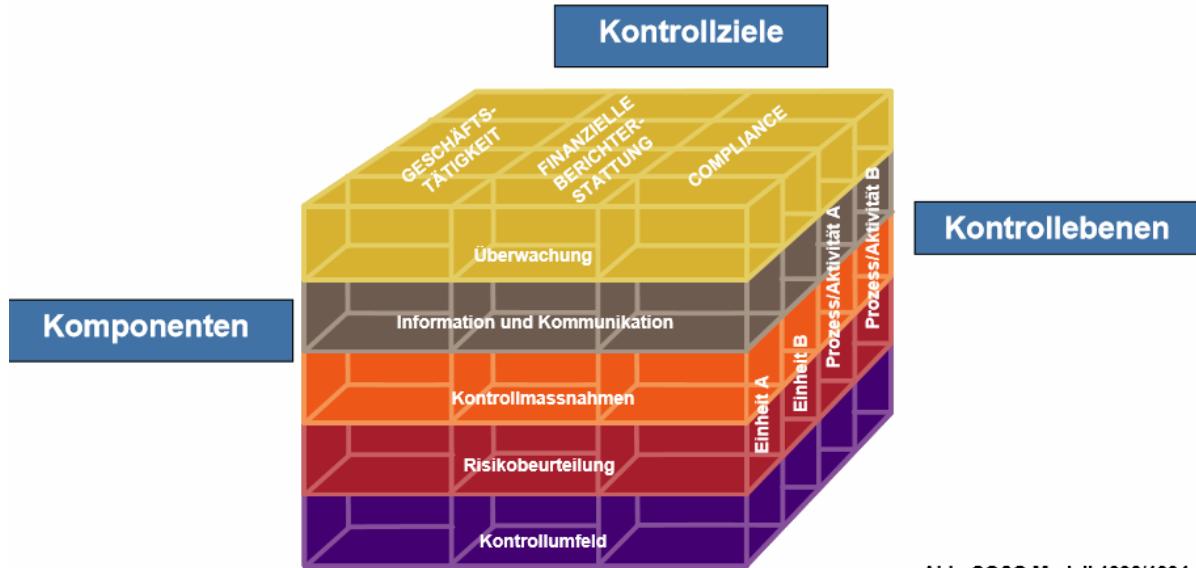


Abb. COSO Modell 1992/1994

#### 9.3.1.1 Kontrollziele

##### **Geschäftstätigkeit (Operations)<sup>1)</sup>**

Effektivität und Effizienz der Unternehmenstätigkeiten

##### **Finanzielle Berichterstattung = Verlässlichkeit der Rechnungslegung (Financial Reporting)<sup>2)</sup>**

Zuverlässigkeit und Integrität der finanziellen Berichterstattung; unter Berücksichtigung externer Anforderungen (ordnungsmässige Buchführung und Rechnungslegung)

##### **Compliance<sup>1)</sup>**

Einhaltung von Gesetzen, Regulatorien, Verträgen und "Best Practices", welche für das Unternehmen relevant sind (abhängig von externen Faktoren, bspw. Aufsichtsbehörde)

##### **Unternehmensstrategie (Strategy)<sup>3)</sup>**

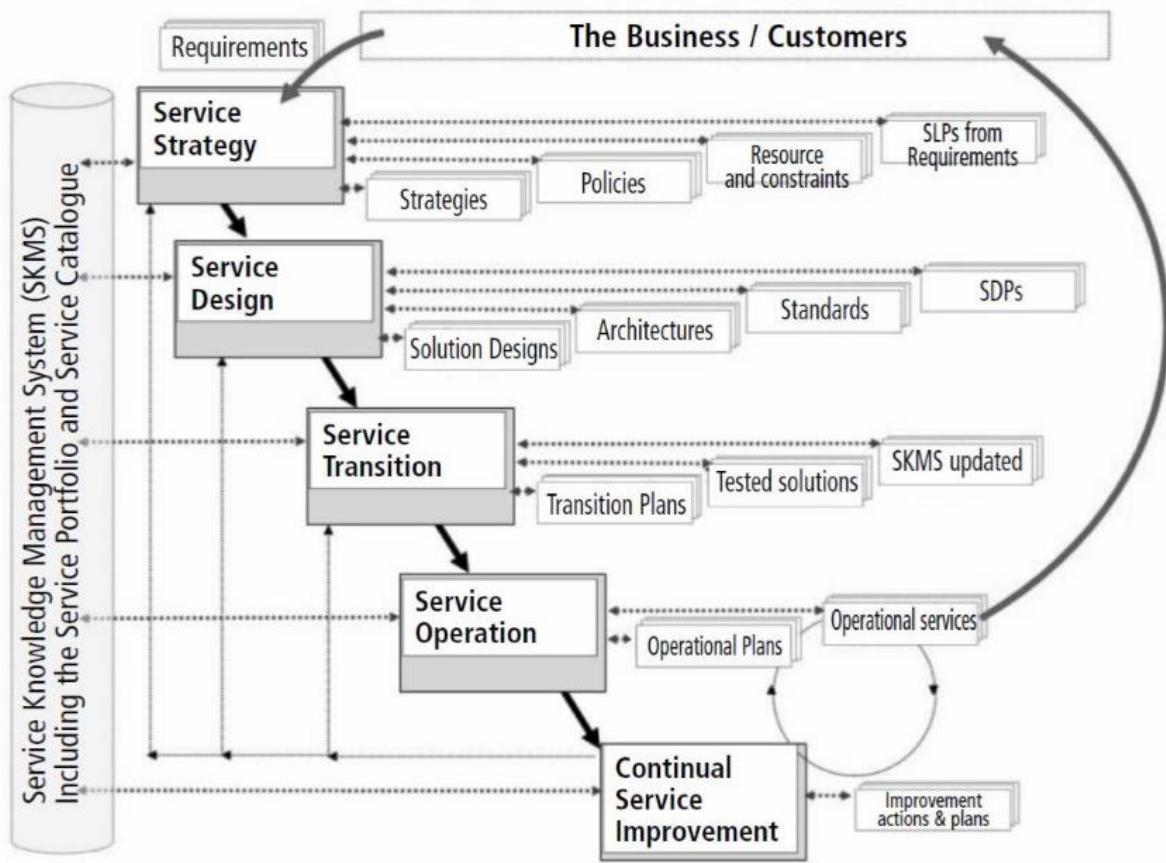
Erstellung einer Unternehmensstrategie; abgeleitet von der Unternehmens-Mission/Vision

1) COSO Modell 1992/1994 und COSO Modell ERM/II

2) Alle COSO Modelle

3) COSO Modell ERM/II

## 9.4 ITIL



## 10 IT-Audit Dokumentation

- Die Dokumentation muss es einem fachkundigen Dritten erlauben, die durchgeführten Prüfaktivitäten, die getroffenen Annahmen sowie die gezogenen Schlüsse nachzuvollziehen
- Wir dokumentieren dies in der Regel in vom Schlussbericht separaten Arbeitspapieren
- Die Arbeitspapiere müssen sämtliche relevanten Unterlagen enthalten, um unsere Schlussfolgerung nachzuvollziehen zu können.
- Dabei werden verschiedene Unterlagen (Evidenzen) in den Papieren querreferenziert analog zu einer wissenschaftlichen Arbeit
- Immer mehr Prüfgesellschaften unterstützen die Dokumentation mit Workflow-Tools und Dokument-Retrositories. Vorteile sind:
  - Zentrale Speicherung von relevanten Unterlagen
  - Erzwingung der Einhaltung von Methodologie und Konsistenz der Dokumentation
  - Ev. vollständig elektronische Archivierung (siehe nächste Folie)
- Klare Nachteile:
  - Oft Restriktionen bezüglich Verfügbarkeit (z.B. nur bei Zugriff auf Firmennetz)
  - Verlust an Flexibilität bezüglich Inhalt

**Ein Arbeitspapier enthält in der Regel folgende Elemente:**

- **Ziele**
- **Durchgeführte Prüfungshandlungen**
- **Schlussfolgerung**
- **Detaillierte Beschreibung Prüfungshandlungen**
  - Prozessbeschriebe
  - Prüfung Design Effectiveness (ToD)
  - Prüfung Operating Effectiveness (ToE)
- **Evidenzenliste**

## 11 Bewertung Ergebnisse

### 11.1 Ineffektive Applikationskontrollen

**Prüfungsergebnisse mit möglichem Einfluss auf Beurteilung:**

- Kontrolle ist in ihrem Design nicht geeignet, die Kontrollziele abzudecken oder wird nicht so ausgeführt, dass die Kontrollziele erreicht werden können
- Geprüfte Kontrollen decken (in ihrer Gesamtheit) Prüfziele für den Prozess nicht ab und es existieren keine Kontrollen, welche mitigierend wirken könnten

**Je nach Kombination der Feststellungen sind die Auswirkungen unterschiedlich zu beurteilen**

**Vorgehen gemäss den im Rahmen der Prüfungsdurchführung besprochenen Möglichkeiten:**

- Beurteilung der Behebung der Kontrollschwäche
- Behebung per welches Datum
- Beurteilung des Einflusses der Kontrollschwäche für die Zeit, in welcher sie bestand (abhängig von der Art der Kontrolle!)
- Identifikation von zusätzlichen Kontrollen, welche mitigierend wirken
- Bestimmung von zusätzlichen, tiefergehenden Prüfprozeduren, um tatsächliche Auswirkungen der Kontrollschwäche zu bestimmen

**Achtung: Bei vollautomatischen Kontrollen liegen Design und operative Effektivität sehr nahe beieinander**

**Kommen wir zum Schluss, dass eine Applikationskontrolle ein Kontrollziel nicht erreicht, stellen sich folgende Fragen:**

- Wird das Prüfziel auch erreicht, wenn wir uns nicht auf diese Kontrolle abstützen können?
- Existieren andere mitigierende Applikationskontrollen, welche wir prüfen könnten, so dass das Prüfziel erreicht wird?
- Existieren mitigierende manuelle Kontrollen, welche wir prüfen könnten, so dass das Prüfziel erreicht wird?
- Können wir ergebnisorientierte Prüfungshandlungen im Prozess durchführen, welche uns auch genügende Sicherheit über das Prüfziel geben?

**Falls alle Fragen mit Nein beantwortet werden müssen, so bleibt uns nichts anderes übrig, als den Prüfansatz für das entsprechende Prüfziel zu verändern und in den meisten Fällen zu einem ergebnisorientierten Prüfansatz zu wechseln. Dies bedeutet in häufig:**

- Zusatzaufwand für Aufsetzen neue Prüfung
- Massiv höherer Aufwand für die eigentliche Prüfung

## 11.2 Ineffektive GITC

**Werden die Generellen IT Kontrollen für eine bestimmte Applikation als gesamthaft nicht effektiv beurteilt so hat dies folgende Auswirkungen:**

- Auch wenn die unterstützte Applikationskontrolle als effektiv beurteilt wurde können wir keine Aussage über das ganze Jahr machen
- Ein Ausweg besteht eventuell, falls wir an einer bestimmten Ausführung der Applikationskontrolle interessiert sind.
- In diesem Fall kann genau diese Ausführung geprüft werden, um angemessene Sicherheit über das Funktionieren der Applikationskontrolle zu erhalten
- Beispiel: Vollständigkeit und Korrektheit eines Reports aus dem System – Falls wir genau denjenigen Report im richtigen Zeitpunkt prüfen, welcher die Grundlage für weitergehende Prüfungshandlungen ist, so kann dies ausreichend sein.

**Falls keine der obigen Auswege anwendbar ist, kann die unterstützte Applikationskontrolle für unsere Beurteilung nicht mehr verwendet werden, und es kommt das auf den vorhergehenden Folien beschriebene Vorgehen bei ineffektiven Applikationskontrollen zur Anwendung**

**Wird eine einzelne Generelle IT Kontrolle als nicht effektiv beurteilt, so hängt der Einfluss dieser Kontrollschwäche auf unsere Gesamtbeurteilung von verschiedenen Faktoren ab:**

- Existenz von kompensierenden Kontrollen auf GITC Ebene (z.B. regelmässiger Rechte-Review kompensierend für Schwäche bei Benutzeradministration)
- Relevanz der Kontrolle für das Prüfziel des GITC Bereichs als ganzes
- Ergebnis von zusätzlich durchgeföhrten (ev. ergebnisorientierten) Prüfaktivitäten
- Direkter Einfluss der Kontrollschwäche auf das Funktionieren der durch sie unterstützten Applikationskontrolle (z.B. Einfluss einer Schwäche bei der Benutzeradministration bei einer Kontrolle, welche nur als Batch ausgeführt wird)

**In allen Fällen müssen wir die Ergebnisse dieser Risikobeurteilung in unseren Arbeitspapieren dokumentieren, so dass ein sachkundiger Dritter unsere Entscheidung nachvollziehen kann**

## 12 Herleitung Massnahmen

**Aus unseren Ergebnissen müssen die Feststellungen klar ersichtlich sein. Feststellungen werden in der Regel folgendermassen strukturiert:**

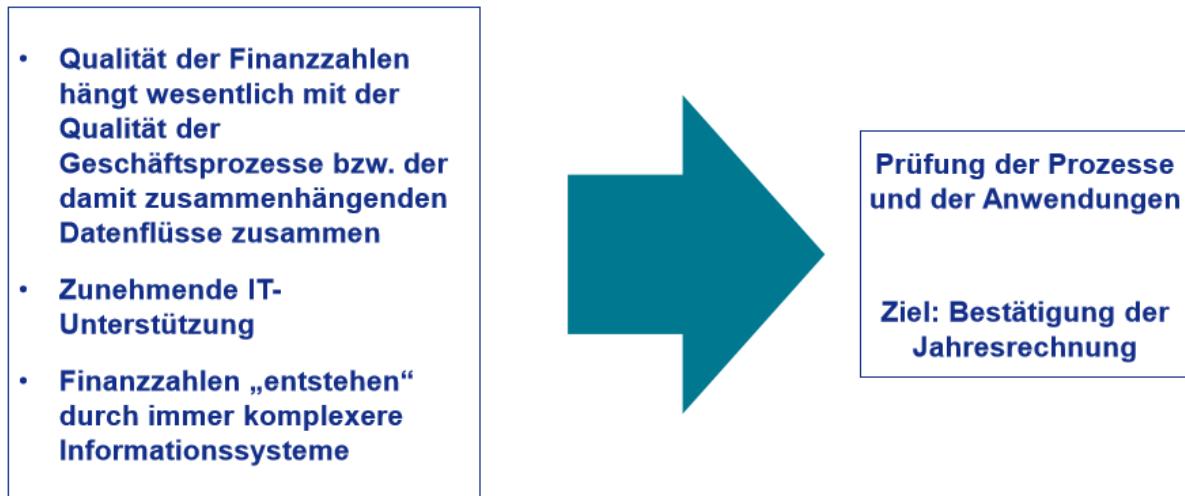
Inhalt	Beispiel
Ausgangslage	Firma XY verfügt seit 2014 über einen formalisierten Prozess zur Vergabe von Benutzerberechtigungen. Rechte müssen dabei vom Vorgesetzten auf einem Papierformular beantragt und mit Datum / Unterschrift bestätigt werden.
Sachverhalt	In unserer Stichprobe von 40 Antragsformularen haben wir festgestellt, dass bei 20 Formularen die Unterschrift durch den Vorgesetzten nicht vorhanden war.
Risiko	Dies birgt das Risiko, dass Benutzern Rechte vergeben wurde, welche sie nicht benötigen und mit diesen die bestehenden Kontrollen in den Geschäftsprozessen umgehen können.
Empfehlung	Wir empfehlen deshalb, dass die Einhaltung des formalisierten Prozesses vollständig durchgesetzt wird.

**Der Weg von einer festgestellten Ausnahme bis zur akzeptierten Feststellung im Bericht kann sehr lang sein**

- Manager werden in ihren Zielen oft auch daran gemessen, dass sie keine Feststellungen von der externen und internen Revision für ihren Bereich haben
- Oftmals werden mehrere Managementstufen nacheinander ihr Einverständnis zu den Resultaten geben müssen
- Es ist deshalb wichtig, dass Feststellungen immer faktisch korrekt und auch neutral formuliert sind
- In der Regel wird vom Manager, welcher die Verantwortung für eine Feststellung übernimmt, eine Stellungnahme mit folgendem Inhalt verlangt:
  - Akzeptanz der Feststellung (Agreed,...)
  - Kurzbeschrieb der geplanten Gegenmassnahmen
  - Fristansetzung für die Gegenmassnahmen

## 13 Vorgehensmodell Anwendungsprüfung

### 13.1 Grundidee



Zweck	Umfang	Anwenderkreis
<b>Integrierter Prüfungsansatz von Prüfer und IT-Prüfer</b>  <i>„Ein integrierter Prüfungsansatz von Prüfer und IT-Prüfer stellt sicher, dass bei anwendungsabhängigen verfahrensorientierten Prüfungen alle wichtigen Gebiete ausreichend abgedeckt werden und „gleichzeitig“ diejenigen IT-spezifische Gebiete geprüft werden, die ebenfalls einen primären Einfluss auf das Prüfziel des Prüfers haben.“</i>	<b>Beschränkt auf die Prüfung von Anwendungen innerhalb eines Geschäftsprozesses</b>  aber:  <i>„Die Anwendung des Vorgehensmodells ist nicht beschränkt auf die Prüfung der Ordnungsmässigkeitskriterien; vielmehr wurde das Vorgehen bewusst generisch gehalten und kann somit auch für andere Prüfungen (z.B. Compliance-Prüfungen) herangezogen werden.“</i>	<b>Auf Abschlussprüfung ausgerichtet</b>  <i>Die Beispiele und Vorgehensbeschreibung sind auf die Abschlussprüfung ausgerichtet. Aufgrund seines generischen Charakters ist das Vorgehensmodell sowohl vom Abschlussprüfer als auch vom IT-Prüfer anwendbar.</i>

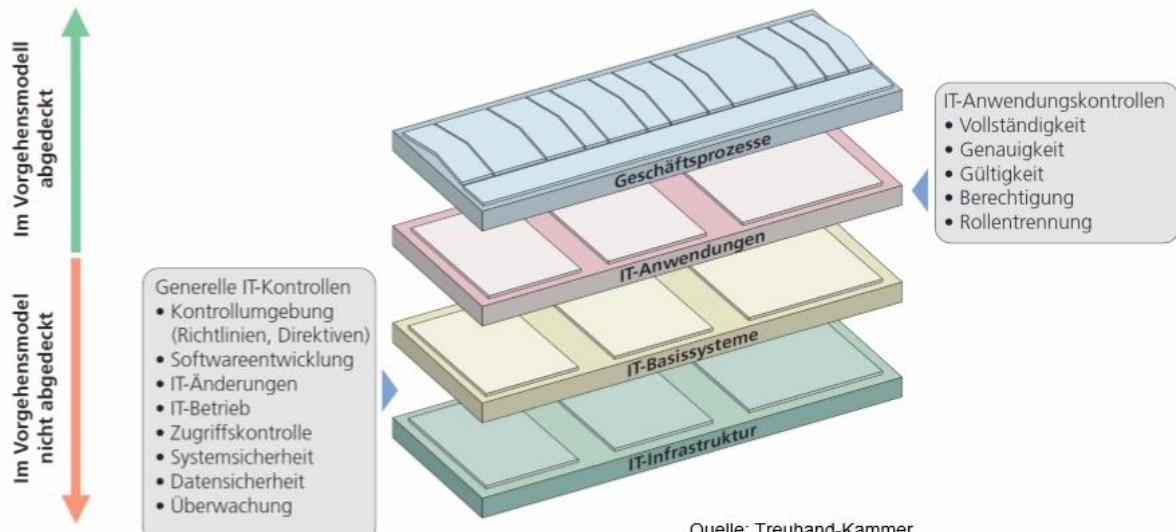
## 13.2 8 Schritte



### Ziel: Testierung der finanziellen Rechnung.

- Eignet sich für die IT Prüfung der Finanzberichterstattung
- Generisches Vorgehen für die Abdeckung von IT Risiken
- Top Down Ansatz zur Identifikation der zu prüfenden Bereiche
- Folgt einem verfahrensorientierten Prüfansatz

Verfahrensorientiert	Ergebnisorientiert
Prüft Effektivität von Kontrollen in Prozessen	Stimmt Belege (Zahlen) miteinander ab
Kann für alle Größen angewendet werden	Nur für sehr kleine Unternehmen



### 13.2.1 1. Analyse

#### **Ziel:**

##### **Identifikation der relevanten Konten bzw. Kontengruppen**

- identifiziert die Risiken, die einen Einfluss auf die zu prüfende Jahresrechnung haben können => Ausrichtung der Prüfstrategie (unter Berücksichtigung der Wesentlichkeitsgrenze)
- Zuordnung der wesentlichen Positionen zu den Geschäftsprozessen

##### **Identifikation der relevanten Transaktionen**

- Sind die Konten-Positionen identifiziert, kann der Prüfer in einem zweiten Schritt analysieren, durch welche Transaktionen deren Bestände massgeblich beeinflusst werden.

### 13.2.2 Geschäftsprozesse & Datenflüsse

#### **Ziel: Identifizierung und Dokumentation der relevanten Geschäftsprozesse**

Ziel dieses Schrittes ist zu verstehen, wie relevante Informationen und Daten fliessen. Dabei geht es nicht nur um elektronische Daten; eine ausreichende Analyse berücksichtigt auch Dokumentenflüsse (zum Beispiel Bericht über Lagerbewertung) und manuelle Schnittstellen

### 13.2.3 Kernanwendungen und der IT-relevanten Schnittstellen

#### **Ziel: Identifikation der beteiligten IT- Anwendungen und deren Schnittstellen.**

Pro Anwendung werden die Merkmale identifiziert. Die daraus hergeleiteten Risiken (Punkt 4) sind die Basis für die detaillierte Definition des Prüfungsumfangs

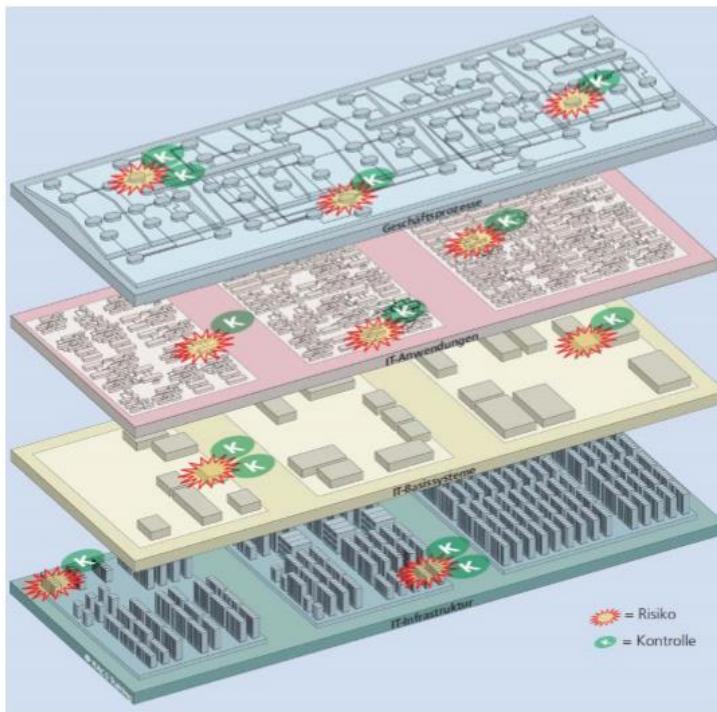
### 13.2.4 Risiken und Schlüsselkontrollen

#### **Ziel: "Kontroll-Universum" abstecken**

Identifizierung der Risiken (Schadensszenarien).

Pro Risiko werden

- die Kontrollen festgehalten um das Risiko zu mitigieren
- Der Einfluss auf die Aussagen im Abschluss analysiert



Identifikation der Risiken und der Kontrollen soll eine effiziente Prüfung ermöglichen.

### 13.2.5 Walk-Through

**Ziel:** Überprüfung des erworbenen Verständnisses über den betreffenden Prozess, die enthaltenen Risiken und Kontrollen und somit auch der Bestätigung der vorhergehenden Analyse.

Anhand einer exemplarischen Transaktion werden manuelle oder automatische Schritte des Prozesses durchlaufen und dokumentiert.

### 13.2.6 Beurteilung des Kontrolldesigns

**Ziel:** Vertieftes Verständnis des Kontroll-Designs

Untersuchung, ob das integrale Interne Kontrollsysteem auf seine Eignung und Wirtschaftlichkeit geeignet ist (Design Effectiveness)

### 13.2.7 Beurteilung der Umsetzung der Kontrollen

**Ziel: Der Prüfer kann ein Urteil über das IKS abgeben**

- Funktioniert eine Kontrolle gemäss ihrem Design,
- Wurde sie tatsächlich durchgeführt
- Wurde sie vollständig durchgeführt
- Wurde sie durch eine qualifizierte und berechtigte Person ausgeführt wurde

### 13.2.8 Gesamtbeachtung und Ergebnisfindung

**Ziel: Abschliessende Aussage, ob das Interne Kontrollsysteem geeignet ist, wesentliche Fehler im Abschluss mit angemessener Sicherheit zu vermeiden**

## 14 Notizen zu Prüfungsfragen Controlls etc

Welche Kontrolltypen definiert die Expert-Suisse: Entity Level Controls, Prozess Kontrollen, Generelle IT Kontrolle.

Was versteht man unter dem Schichten Modell der Expert Suisse: Dieses Schichtenmodell definiert die Zusammenhänge zwischen den Kontrollen innerhalb eines Audits. Für den Audit der Finanzbericht erstattung. Ziel des Modells ist die Jahresrechnung.

Case 4-5-6: Kontrollen identifizieren --> Alle 2 Sätze eine Kontrolle ca. Pro Satz max 1 Kontrolle.  
Einfach den Satz markieren und dann Kontrolle schreiben.

Das Unternehmen nutzt für seine Finanzbuchhaltung Applikation X --> Keine Kontrolle

Das Cobit-Team stellt sicher, dass die Finanzbuchhaltung die Kontrollen umsetzt --> Entity Level -->  
Betrifft das ganze Unternehmen und mehrere Bereiche / Applikationen

Zugangsberechtigungen --> Generelle IT Kontrollen "Access" immer Generelle IT-Kontrolle  
Wenn Kontosätze konfiguriert sind, dass bestimmte Dinge sich ändern --> Prozess Kontrolle

Was ist der Zusammenhang zwischen Applikations und Generellen IT-Kontrollen: Wenn die ITGC wegfallen, dann kann ich immer noch etwas zu den Applikationen sagen. "Zu dem Zeitpunkt wo ich getestet habe, gab die IT-Applikation eine korrekte Aussage." DER ZEITBEZUG ist hier relevant. "Die Aussagen waren fürs ganze Jahr relevant stimmt nur wenn ITGC stimmen."  
Weiter Auswirkung auf die Prozesskontrollen.

Stichprobengrösse: Eine Bank macht etwas mit Tagesverarbeitungen um Zinssätze zu ermitteln.  
Automatische Kontrolle --> Automatische Berechnungen --> Sample of 1  
Wenn es Aussnahmen gibt bei einem automatischen z.b. eine Aussteuerung muss 2x pro Tag Manuell ausgeführt werden --> Multiple Times per Day --> 25-40 und für den automatischen ein SO1

Wenn der Prozess zwischen internen und externen nicht unterscheidet --> Zusammenziehen --> Uns interessieren die Eintritte --> Kündigungen ignorieren.

Was passiert, wenn 2 Stichproben schiefgehen. --> Resampling erneut testen. Macht das Resampling überhaupt Sinn oder ist der Fehler so gravierend, dass es sowieso keinen Sinn macht? "Sind die Ausnahmen akzeptabel oder nicht"

Unterschied zwischen ITIL und COBIT. ITIL --> Prozesse best practice. COBIT Kontroll-Framework. ITIL -> TopDown COBIT BOTTOM UP

Change und Accessmanagement nicht ok --> was heisst das für uns als IT-Prüfer bezüglich den Prozess-Kontrollen?

1. Sind Kontrollen betroffen? Habe ich Prozess Kontrollen?
2. Ich suche nach kompensierenden Kontrollen --> z.b. Logs um die Schwäche zu beheben
3. Prüfansatz ändern zu einem Ergebnisorientierten Prüfansatz? --> Jeder Beleg wird durchgeschaut.