

Zusammenfassung IT-Audit

Studium: 6. Semester Bachelor Wirtschaftsinformatik an der Hochschule Luzern

Autor: Janik von Rotz (<https://janikvonrotz.ch>)

Inhalt

1	IT-Governance	1
1.1	COBIT 5	2
2	Wertbeitrag IT	4
2.1	Einfluss der IT auf Umsatz und Kosten	4
2.2	Elemente des IT-Kostenmanagements.....	5
2.3	Geschäftsprozesse	5
2.4	Portfolioanalyse - Chancen- und Risiko-Portfolio.....	5
3	Digital Business.....	7
3.1	5-Kräfte-Modell und digitale Transformation	7
3.2	Ansatzpunkte für die Digitalisierung	7
3.3	Veränderung der Geschäftswelt.....	8
3.4	Digitale Transformation in 3 Dimensionen.....	8
3.5	Organisatorische Veränderung.....	9
3.6	Referenzmodell digitale Transformation.....	9
3.7	Vorgehen und Empfehlungen zum digitalen Wandel	10
3.8	Zusammenfassung Chancen und Risiken	10
4	Wirtschaftlichkeitsanalyse.....	11
4.1	Business Case.....	11
4.2	Bausteine eines Business Cases.....	11
4.3	Investitionsentscheid.....	12
4.4	Business-Case-Erstellung.....	12
4.5	Business Case Dokumentation	13
4.6	Business Case für Social Media.....	14
4.7	Kennzahlen	14
5	Outsourcing	15
5.1	Begriffsdefinition	15
5.2	Fragestellungen	15
5.3	Outsourcing Scope und Formen	15
5.4	Bewertung Outsourcing-Kandidaten.....	16
5.5	Argumente zum Outsourcing	17
5.6	Beispiel Lösungsbewertung	18
5.7	Erfolgsfaktoren	18
5.8	Outsourcing-Prozess.....	19
5.9	Service-Level-Agreements (SLA).....	19
5.10	Chancen und Risiken IT-Outsourcing.....	19

6	Vali IT	20
6.1	Tourismus Branche im Wandel	20
6.2	Spannungsfeld zwischen Innovation und Kostendruck.....	20
6.3	Einführung Val IT	21
6.4	Kritische Würdigung Val IT	22
6.5	Zusammenfassung.....	22
7	Lizenzmanagement.....	23
7.1	Begriffsdefinitionen	23
7.2	Einführung Lizenzmanagement.....	23
7.3	Software Life Cycle	24
7.4	Rolle Lizenzmanager	24
7.5	Zusammenfassung.....	24
8	IT-Audit	25
8.1	Vorgehensmodell Anwendungsprüfung.....	25
8.2	Revisionsplanung.....	25
8.3	Prüfungs durchführung.....	26
8.3.1	Entity Level Controls (ELC).....	26
8.3.2	Process Level Controls.....	27
8.3.3	Generelle IT Kontrollen.....	27
8.3.4	Prüfprozeduren.....	27
8.3.5	Manuelle Kontrollen.....	28
8.3.6	Automatische Kontrollen.....	29
8.3.7	Verhalten bei Exceptions.....	29
8.3.8	Attestation Reports	30
8.3.9	End User-Computing (EUC).....	30
8.4	IT Audit Frameworks	31
8.4.1	ISACA	31
8.4.2	COBIT	31
8.4.3	COSO.....	32
8.5	Ergebnisbewertung	32
8.5.1	Dokumentation.....	32
8.5.2	Bewertung	33
8.5.3	Inneffektive Generelle IT Kontrollen (Gesamthaft)	33
8.5.4	Inneffektive Generelle IT-Kontrolle (Einzeln)	34
8.6	Herleitung Massnahme	34
8.7	Vorgehensmodell	35

9	Verzeichnisse	36
9.1	Abbildungsverzeichnis	36
9.2	Begriffsverzeichnis	37

Legende:

: Ergänzung

<> Konflikt

-> Folge

/ Oder

~ Beispiel

1 IT-Governance

- Steuern, Regieren
- Rolle
- Compliance -> Audit

Ein Vergleich mit der Staatsform:



Beispiel:

- Policy: Wir schützen unsere Endgeräte
- Standards: Technisches Produkt
- Guidelines: Tipp & Tricks
- Procedures: Checklisten

IT-Controlling wird vom Management aufgebaut.

- Planung
- Steuerung
- Informationsbereitstellung

IT-Audit regelt die Compliance nach innen und aussen.

IT-Prefix schränkt lediglich den Betrachtungsgegenstand ein.

Formen der Richtungsvorgabe:

- Guidelines
- Richtlinien

Management-Funktion

- Align, Plan and Organise (APO): Anpassen, Planen und Organisieren
- Build, Acquire and Implement (BAI): Aufbauen, Beschaffen und Implementieren
- Deliver, Service and Support (DSS): Bereitstellen, Betreiben und Unterstützen – Monitor, Evaluate and Assess (MEA): Überwachen, Evaluieren und Beurteilen

Der Management Prozess ist natürlich iterativ gekoppelt.

Die Strategiebildung ist Teil der Evaluation und Richtungsvorgabe.

Ausprägung ist sehr unterschiedlich.

GEIT - Governance Enterprise IT

Interne und externe Stakeholder

- Create Value
 - Nutzen
 - Task
 - Ressources
- Enterprise Goals
- IT Goals

1.1 COBIT 5

COBIT 5 besteht aus fünf Prinzipien. Diese sollen gewährleisten, dass das Unternehmen einen Vorteil aus der IT ziehen kann. Diese Grundprinzipien helfen dem Unternehmen die Unternehmensziele zu erreichen. Das Framework zeigt den Firmen auf, was gemacht werden muss um erfolgreich zu sein. Es liefert dabei jedoch keine explizierten Methoden um dies zu bewerkstelligen.

Prinzip 1: Erfüllung der Anforderungen der Anspruchsgruppen

Die Stakeholder bilden die Treiber für die Zielsetzungen. Aus den Anspruchsgruppen-Anforderungen bilden sich die Firmenziele. Daraus lassen sich die IT Zielsetzungen ableiten.

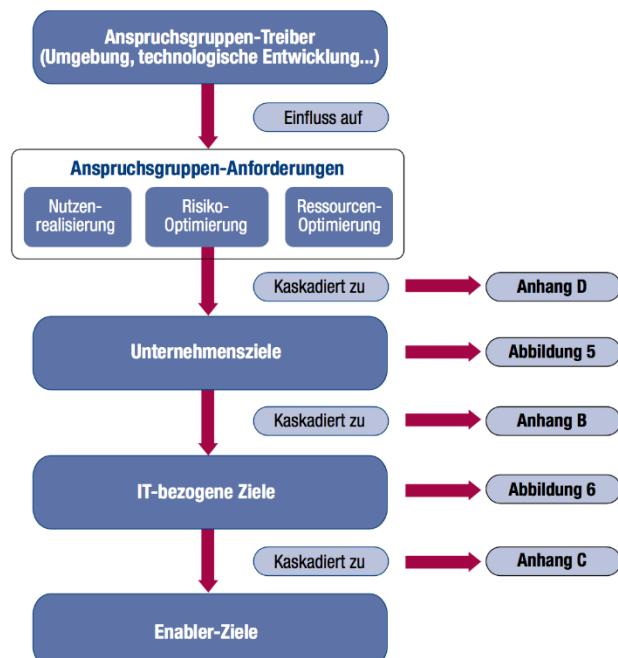


Abbildung 1: COBIT 5 Anspruchsgruppen

Prinzip 2: Abdeckung des gesamten Unternehmens

COBIT 5 deckt alle relevanten Funktionen und Prozessen zu Informationen und Technologien für die Führung eines Unternehmens ab. Es greift dabei auf das Prinzip 1 den Bedürfnissen der Stakeholder zurück.

Prinzip 3: Anwendung eines einheitlichen, integrierten Rahmenwerks

- An andere aktuellen und relevanten Standards und Rahmenwerken ausgerichtet
- Deckt Unternehmen lückenlos ab
- Einfache Architektur

Prinzip 4: Ermöglichung eines ganzheitlichen Ansatzes

COBIT definiert 7 Enabler, welche die Erreichung der Unternehmensziele ermöglichen sollen. Enabler 5 bis 7 sind gleichzeitig Unternehmensressourcen, die es zu managen und zu führen gilt.

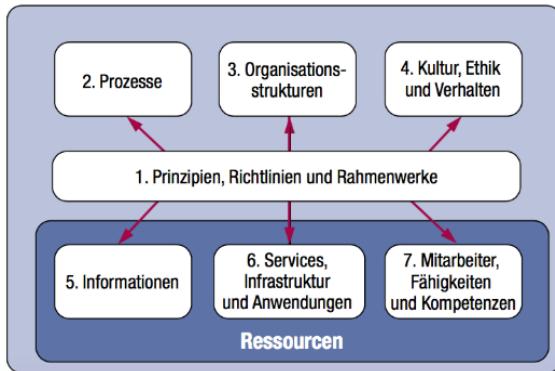


Abbildung 2: COBIT 5 Enabler

Prinzip 5: Unterscheidung zwischen Governance und Management

Ziel ist es die Zielformulierung und Überprüfung von der Umsetzung zu trennen. Das Prozessreferenzmodell unterteilt die Governance- und Managementprozesse in zwei Prozessdomänen.

- **Governance:** Diese Domäne besteht aus fünf Governance-Prozessen. Für jeden dieser Prozesse sind sogenannte EDM-Praktiken definiert (EDM: Evaluieren, Richtung vorgeben und Überwachen)
- **Management:** Diese Domäne besteht aus vier weiteren Domänen, die den Zuständigkeitsbereichen Planen, Aufbauen, Ausführen und Überwachen entsprechen (PBRM: Plan, Build, Run, Monitor) und sorgt für eine lückenlose IT-Abdeckung

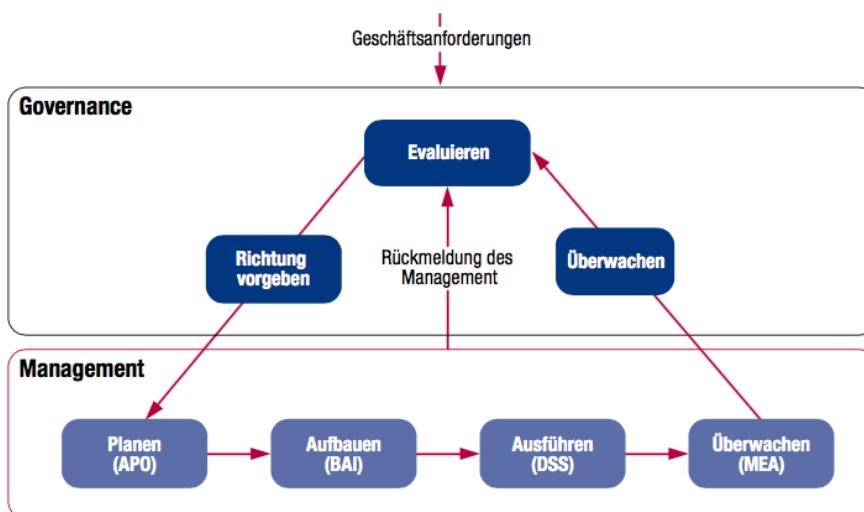


Abbildung 3: COBIT 5 Kernbereich von Governance und Management

APO	Align, Plan and Organise	Anpassen, Planen und Organisation
BAI	Build, Acquire and Implement	Aufbauen, Beschaffen und Implementieren
DSS	Deliver, Service and Support	Bereitstellen, Betreiben und Unterstützen
MEA	Monitor, Evaluate and Assess	Überwachen, Evaluieren und Beurteilen

2 Wertbeitrag IT

IT als strategische Waffe: ein Unternehmen nutzt die IT um einen entscheidenden Vorteil gegenüber der Konkurrenz zu haben

IT als Commodity (IT doesn't matter): Die IT muss lediglich den Bedürfnissen des Business entsprechen. Dadurch sollen die Kosten geringer sein, es kann aber kein Wettbewerbsvorteil gewonnen werden.

2.1 Einfluss der IT auf Umsatz und Kosten

Durch den Einsatz neuer IT besteht die Möglichkeit, die IT-Kosten zu senken. Der grösste Hebel wirkt direkt bei der Optimierung der Geschäftsprozesse. Mit dieser Optimierung lassen sich erhebliche Effizienzgewinne realisieren. Die damit verbundenen Verbesserungen bei den Prozesszeiten und der Prozessqualität wirkt sich positiv auf die Kunden-zufriedenheit aus. Neben den Kosten ist zwingend das Potential auf den Umsatz zu analysieren.

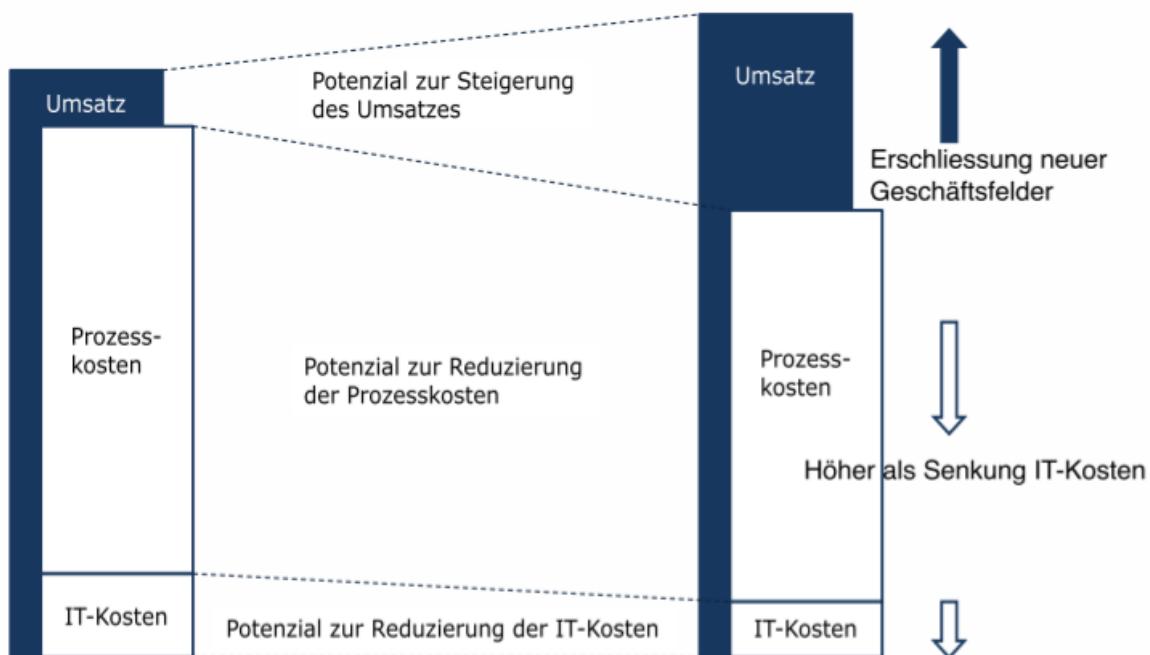
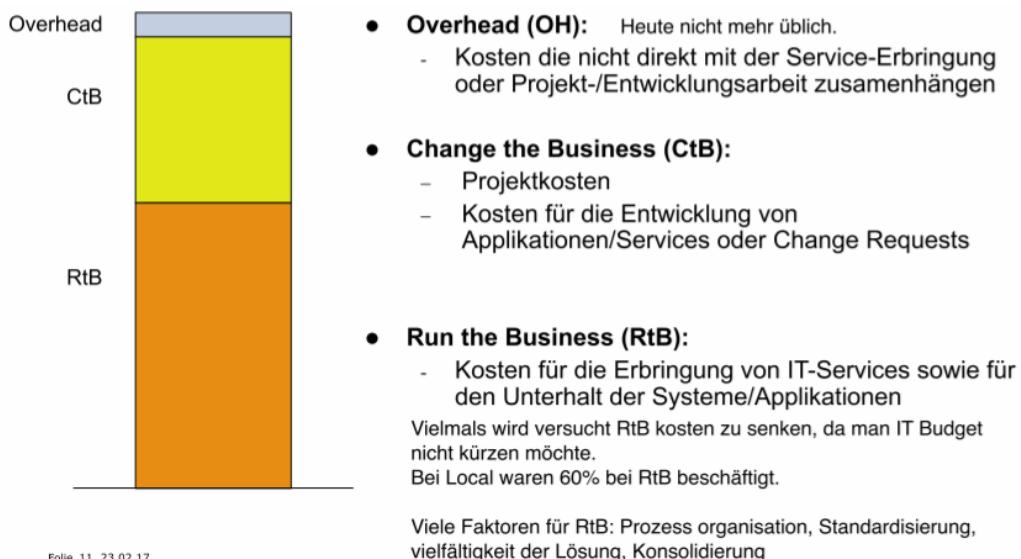


Abbildung 4: Wertbeitrag der IT

IT-Value = IT-Nutzen minus IT-Kosten

2.2 Elemente des IT-Kostenmanagements



Folie 11, 23.02.17

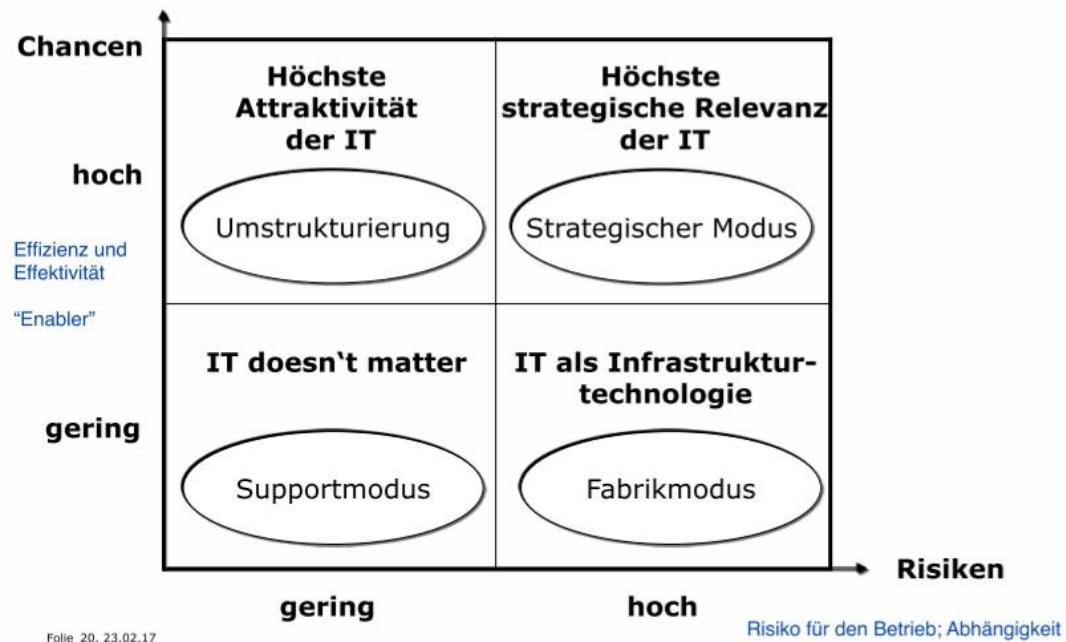
Abbildung 5: Elemente IT-Kostenmanagement

2.3 Geschäftsprozesse

Kennzeichen:

- 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

2.4 Portfolioanalyse - Chancen- und Risiko-Portfolio



Folie 20, 23.02.17

Abbildung 6: Chancen- und Risiko-Portfolio

Supportmodus

- Aufgabenbereiche (IT-Management)
 - Analyse der Veränderung (Veränderung der Chancen oder Risiken im Zeitverlauf)
 - Monitoring der IT-Aktivitäten der Wettbewerber
 - Kosteneffiziente Steuerung der IT-Budgets (Vermeidung von unnötigen Innovationen)
- IT hat eine sehr geringe Bedeutung

Umstrukturierungsmodus

- Aufgabenbereiche (IT-Managements)
 - Sicherstellung des finanziellen Budgets zur Nutzung der Innovationspotentiale
 - Aufstockung des IT-Personals und Finanzen zur Nutzung der Chancen
- Start-Ups sind typisch für diesen Modus

Strategischer Modus

- Aufgabenbereiche (IT-Management)
 - Permanente Abstimmung der IT-Strategie mit der Unternehmensstrategie
 - Analyse der Innovationsfähigkeit der IT-Systeme
 - Herstellung von Transparenz über die IT-Performance der Wettbewerber
- In diesem Modus hat die IT eine grosse Bedeutung und bringt damit auch grosses Risiko

Fabrikmodus

- Aufgabenbereiche (IT-Management)
 - Gewährleistung der Ausfallsicherheit durch redundante IT-Systeme und Datenhaltung
 - Gewährleistung der Datensicherheit durch Vermeidung von Angriffen
- In diesem Fall hat die IT geringes Potential, sie ist allerdings für die Geschäftstätigkeit zentral

3 Digital Business

Disruptive Technologien und innovative Geschäftsmodelle sowie Automatisierung, Flexibilisierung und Individualisierung stehen im Vordergrund.

Industrie 1.0 Mechanik

Industrie 2.0 Elektrizität

Industrie 3.0 Computer

Industrie 4.0 Digitalisierung

3.1 5-Kräfte-Modell und digitale Transformation

Je stärker diese fünf Kräfte ausgeprägt sind, desto schwerer lassen sich für ein Unternehmen Wettbewerbsvorteile in dieser Branche erzielen. Mit den bisherigen Prozessen und Geschäftsmodellen können traditionelle Anbieter zukünftig nicht mehr am Markt bestehen. Um disruptive Innovationen wie dem Auto der Zukunft begegnen und in der Branche weiterhin wettbewerbsfähig zu sein, müssen diese die digitale Transformation in Angriff nehmen.

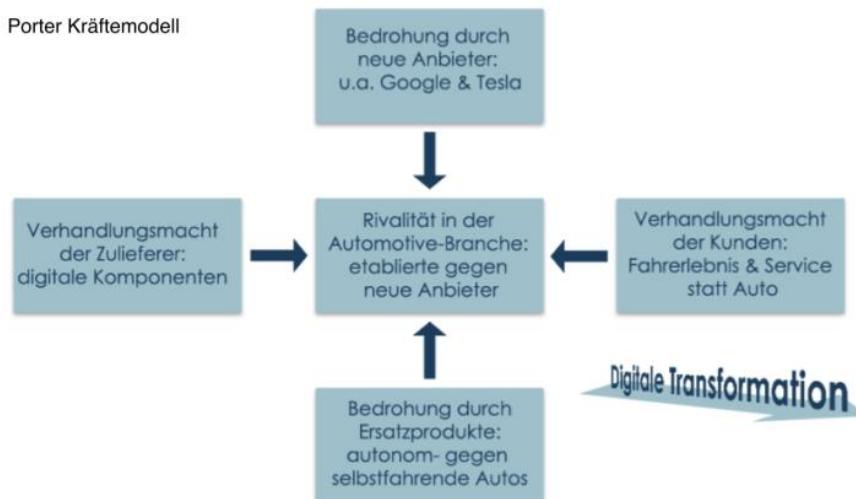


Abbildung 7: Porter Kräftemodell

3.2 Ansatzpunkte für die Digitalisierung

4 Möglichkeiten zum ansetzen.
Können kombiniert werden.

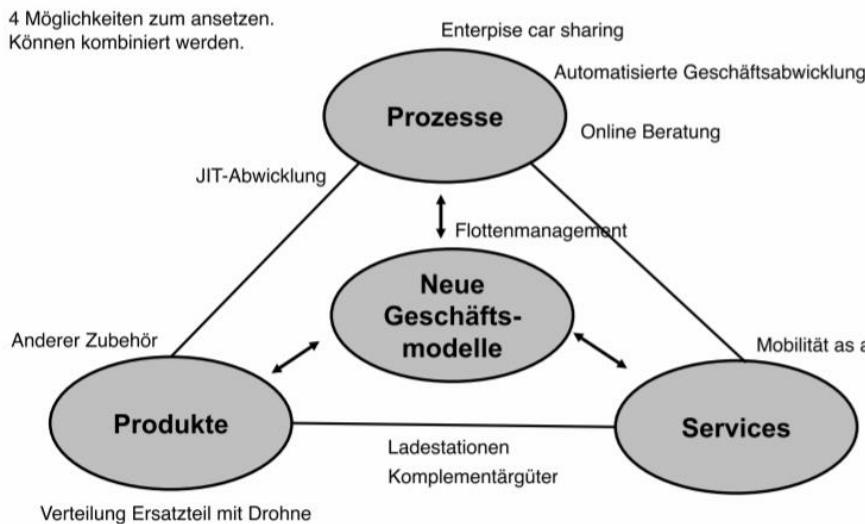


Abbildung 8: Ansatzpunkte für die Digitalisierung

3.3 Veränderung der Geschäftswelt

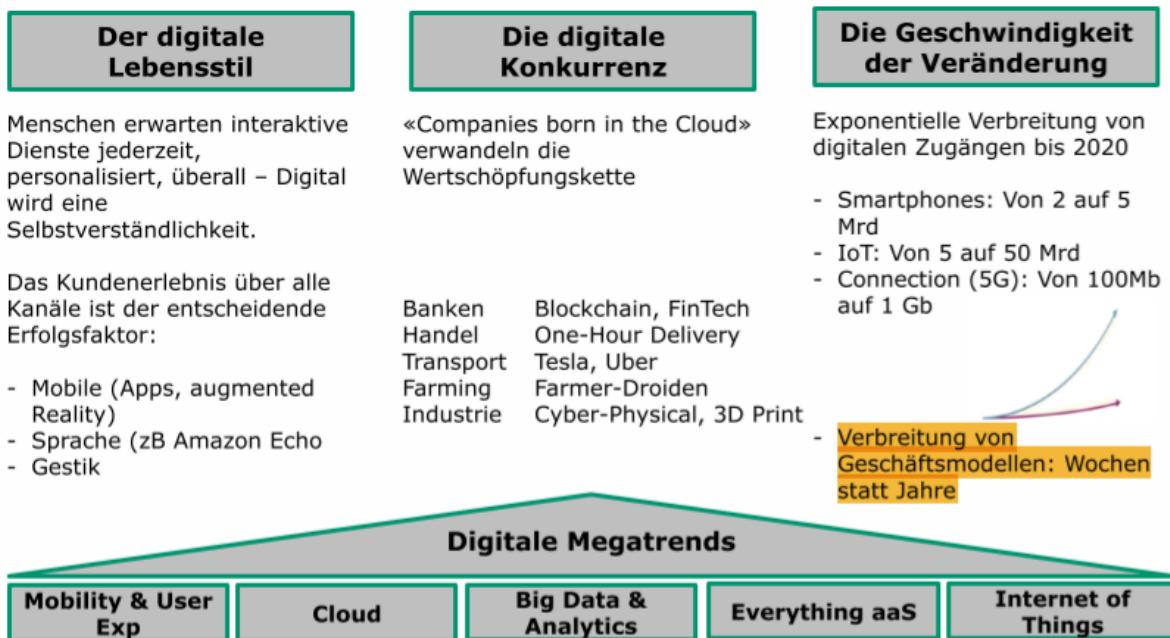


Abbildung 9: Auswirkungen der Digitalisierung auf die Geschäftswelt

60% der Unternehmen in der Schweiz haben sich bereits mit der Digitalisierung auseinandergesetzt.

3.4 Digitale Transformation in 3 Dimensionen

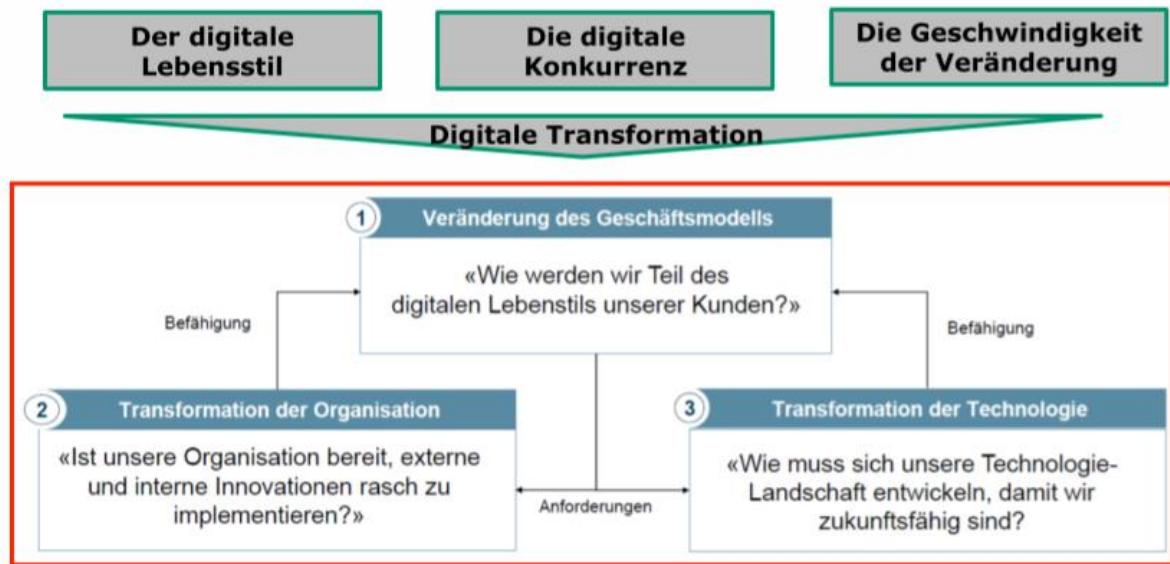


Abbildung 10: Auswirkungen der digitalen Transformation

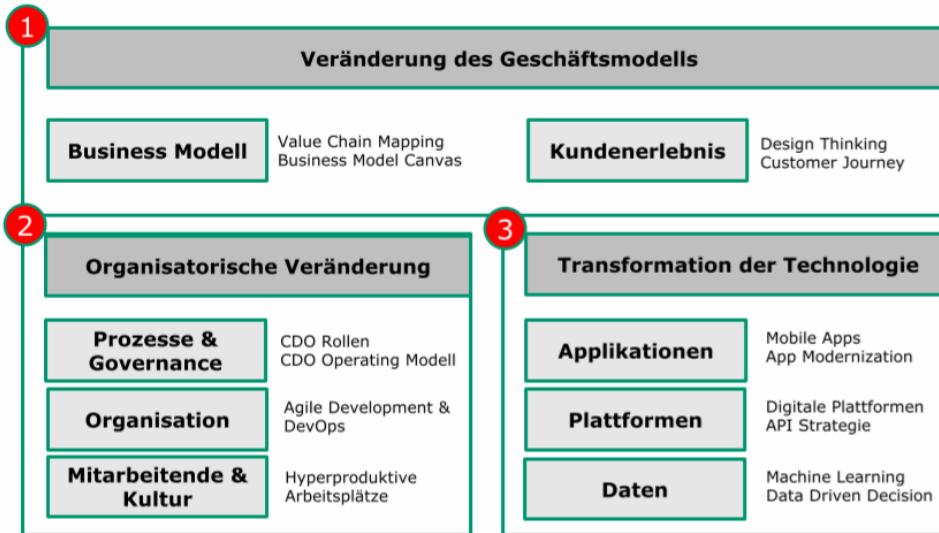


Abbildung 11: Beispiele für die drei Dimensionen

3.5 Organisatorische Veränderung

- Etablierung CDO -> Chief Digital Officer
- Koordiniert ein Innovation Team
- Sind fähig Start-up-ähnliche Struktur zu bilden
- Aufgabenbereich CDO
 - Entwicklung und Umsetzung Digitalstrategie
 - Unterstützung Entwicklung digitaler Lösungen für Geschäftsprozesse
 - Einführung «Best Practices»
 - Förderung Informationsflusses
 - Verwaltung digitales Budget

3.6 Referenzmodell digitale Transformation



Abbildung 12: Referenzmodell digitale Transformation

3.7 Vorgehen und Empfehlungen zum digitalen Wandel

Vorgehen:

1. Schritt: Workshop (Chancen des digitalen Wandels für die eigene Firma)
2. Schritt: Definition von Anwendungsfällen
3. Schritt: Priorisierung der Anwendungsfälle für Entwicklung der Geschäftstätigkeit
4. Schritt: Realisierung von erfolgsversprechenden Kurzprojekten (Exploratives Testen)
5. Schritt: Interne Vermarktung der Erfolge
6. Schritt: Realisierung grundlegende Projekte

Handlungsempfehlungen:

- Technologie als Chance sehen
- Neue Strategien entwickeln
- Digitalisierung aus Kundensicht betrachten (Customer Journey)
- Rollen im Unternehmen neu definieren

3.8 Zusammenfassung Chancen und Risiken

Risiken		Chancen														
<p>Risiken</p> <p>Kanton Genf verbietet Fahrdienst Uber Schweizer Taxifahrer demonstrieren gegen Uber «Wenn nötig, streiken wir» Occupational Number of Workers</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Occupation</th> <th>Number of Workers</th> </tr> </thead> <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>	Occupation	Number of Workers	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>Chancen</p> <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>Folien 26-28</p> <p>«Take Away» Messages:</p> <ul style="list-style-type: none"> • Gleich lange Spiesse, Gesetzgeber hinkt der Entwicklung hinterher • Ethische Aspekte für Gesellschaft mitberücksichtigen! <p>Folien 4-9</p> <p>«Take Away» Messages:</p> <ul style="list-style-type: none"> • Ansatzpunkte für Digitalisierung: Prozesse, Services, Produkte, disruptive Geschäftsmodelle • Geschwindigkeit & Exploration <p>Folien 10-20</p> <p>«Take Away» Messages:</p> <ul style="list-style-type: none"> • Chancen entlang des gewandelten Kundenbedürfnis («Customer Journey») • Potential der neuen Technologien • Neue Denkmuster im digitalen Wandel
Occupation	Number of Workers															
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															

4 Wirtschaftlichkeitsanalyse

4.1 Business Case

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

Beim Business Case gibt es 4 Stakeholder.

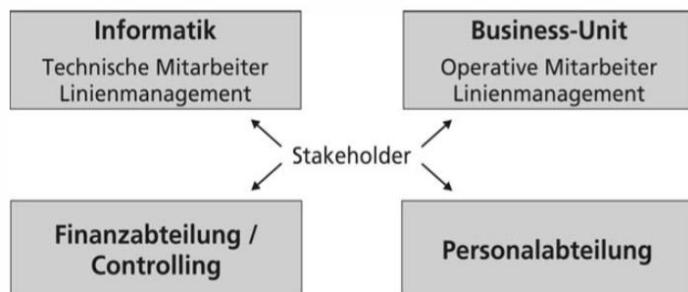


Abbildung 13: Stakeholder Business Case

4.2 Bausteine eines Business Cases

Einsparung muss realisierbar sein.

Im Rahmen der Business Case – Erstellung werden alle Kostenfaktoren und alle Nutzenaspekte für ein spezifisches Projekt erhoben, quantifiziert und dokumentiert.

Obwohl das wirtschaftliche Belangen im Mittelpunkt stehen, werden in einem Business Case neben den rein finanziellen Größen auch alle nicht-monetären Aspekte des Projekts gewürdigt.

Dies sind vor allem Abwägung hinsichtlich Risiken und Strategieorientierung in Verbindung mit den jeweiligen Optionen und deren wirtschaftlichen Vorteilhaftigkeiten.

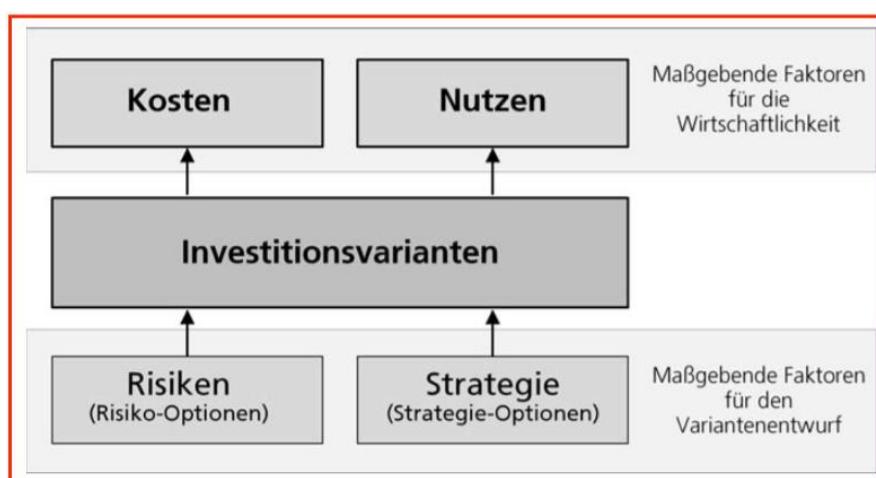


Abbildung 14: Bausteine Business Case

4.3 Investitionsentscheid

Business Cases können im Hinblick auf die Erstellung in zwei Arten unterschieden werden.

- **Durchführungsentscheidung - Absolute Vorteilhaftigkeit:** Ist das zur Entscheidung anstehende Projekt vorteilhaft oder nicht?
- **Auswahlentscheidung - Relative Vorteilhaftigkeit:** Welche Investitionsalternative ist vorteilhafter?

4.4 Business-Case-Erstellung

Phasen:



Abbildung 15: 3 Phasen der BC-Erstellung

Vorgehen:



Abbildung 16: BC Vorgehensmodell

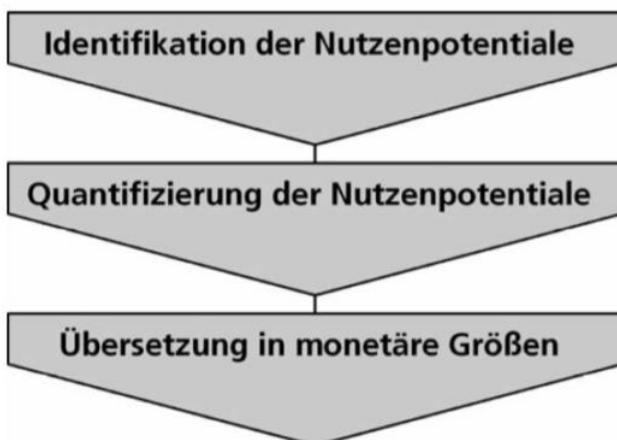


Abbildung 17: Festlegung des Nutzens



Abbildung 18: BC Nutzenkategorien

4.5 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)

4.6 Business Case für Social Media

Aufbau einer Kunden-Community steht im Zentrum.

Investitionen ins Social Media wurde in den vergangenen Jahren von vielen Unternehmen getätigt. Dabei stellt sich die Frage, wo der genaue Nutzen ist, was es Kostet was für Möglichkeiten es gibt und was die Risiken sind. Am Ende sollte klar sein, was der wirtschaftliche Effekt einer solchen Investition ist.

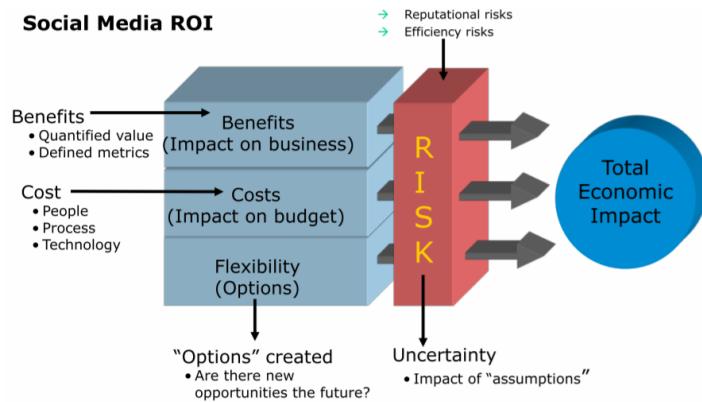


Abbildung 19: Social Media ROI

Nutzen für den Support

- Kosteneinsparung ~durch weniger Kundenanfragen über Telefon
 - Community lösen Probleme anderer Kunden
 - Service kann die Erkenntnisse der Community nutzen
- Einnahmesteigerung durch verbesserte Kundenzufriedenheit

Nutzen für den Rest der Firma

- Product Development durch neue Ideen der Community
- Marketing und Sales durch Mund-zu-Mund-Propaganda

Kosten:

- Ausbildung und zusätzliches Personal
- Kommunikationsmarketing z.B. Richtlinien für Social Media
- Technologie wie Reporting, Analytics, Plattform

4.7 Kennzahlen

NPV: Net Present Value Nutzen über Betrachtungsdauer
Diskontierung von Kosten und Nutzen
Differenz über Betrachtungsdauer

«Was bleibt nach Abschluss der Betrachtungsdauer»

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

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

Pay Back/Break Even

«In welchem Jahr komme ich in die Gewinnzone»

5 Outsourcing

5.1 Begriffsdefinition

Der Begriff „Outsourcing“ ist ein Kunstwort aus den Wörtern „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.

5.2 Fragestellungen

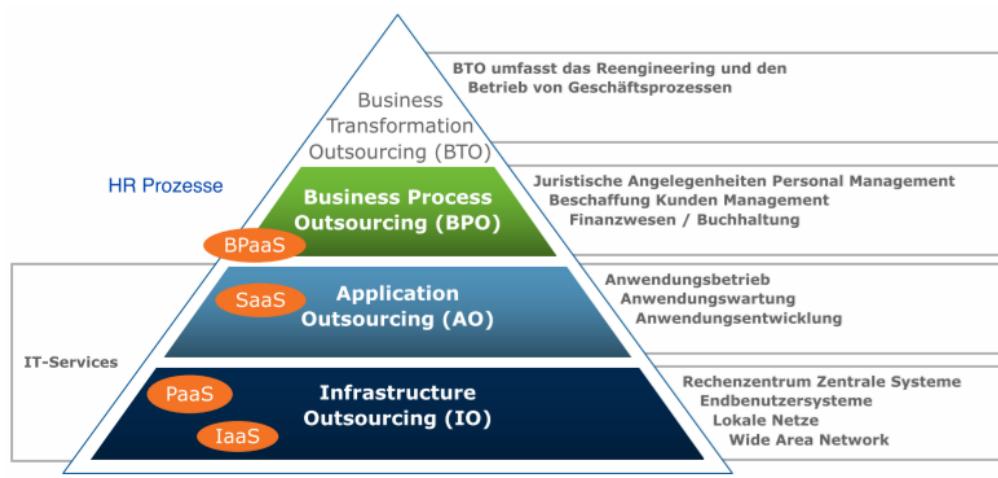
Scope

- 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?

5.3 Outsourcing Scope und Formen



Cloud Servicemodelle
 BPaaS: Business Process as a Service
 SaaS: Software as a Service
 PaaS: Plattform as a Service
 IaaS: Infrastructure as a Service

Cloud Organisationsformen
 Private Cloud
 Community Cloud
 Public Cloud
 Hybrid Cloud

Abbildung 20: Outsourcing Scope und Formen

5.4 Bewertung Outsourcing-Kandidaten

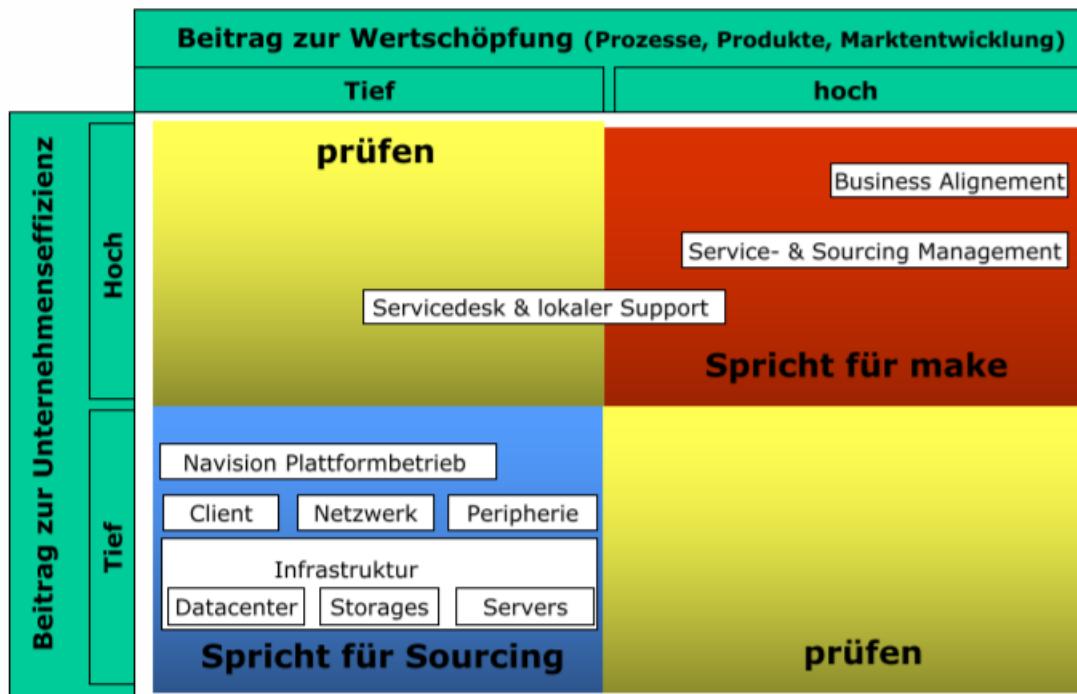


Abbildung 21: Outsourcing-Bewertung - Unternehmenseffizienz und Wertschöpfung

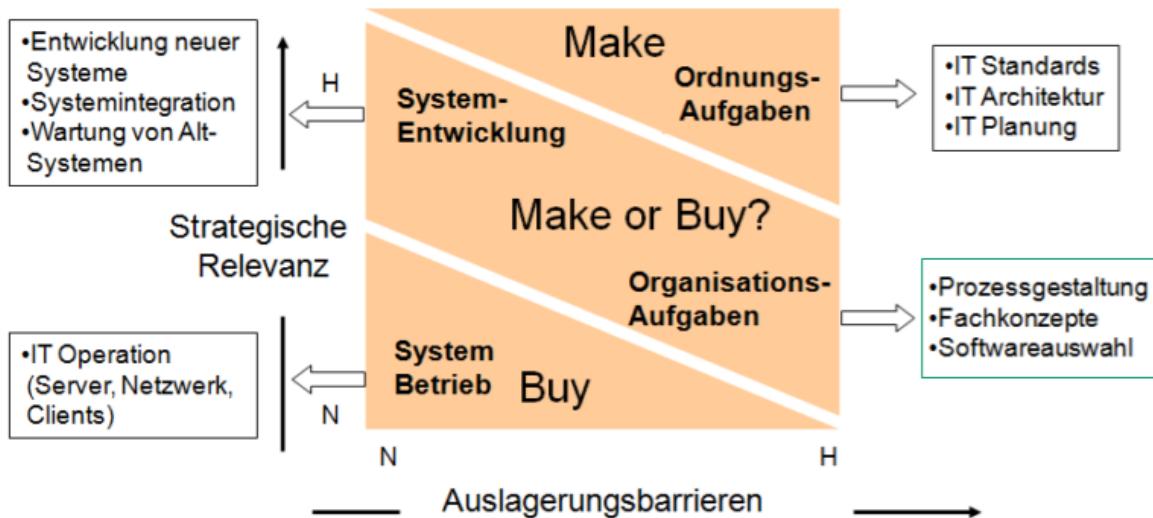


Abbildung 22: Outsourcing-Bewertung - Strategische Relevanz und Auslagerungsbarrieren

5.5 Argumente zum Outsourcing

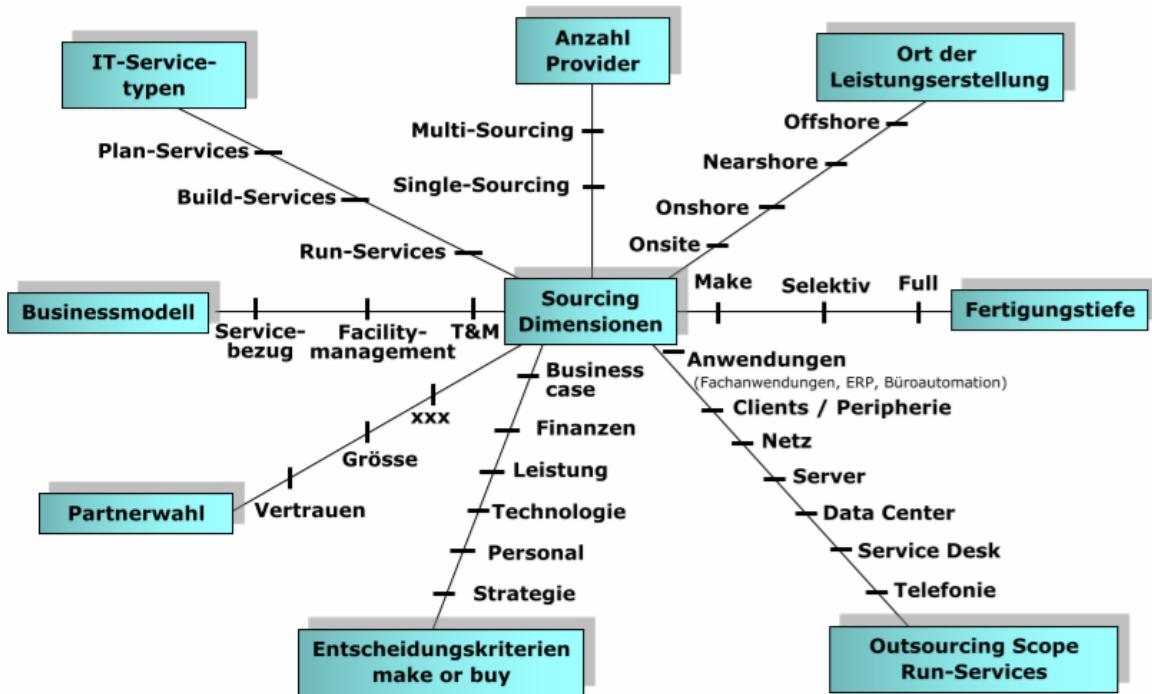


Abbildung 23: Sourcing Dimensionen

5 Kriterien-Gruppen:

1. Strategie
2. Leistung
3. Kosten
4. Personal
5. Finanzen

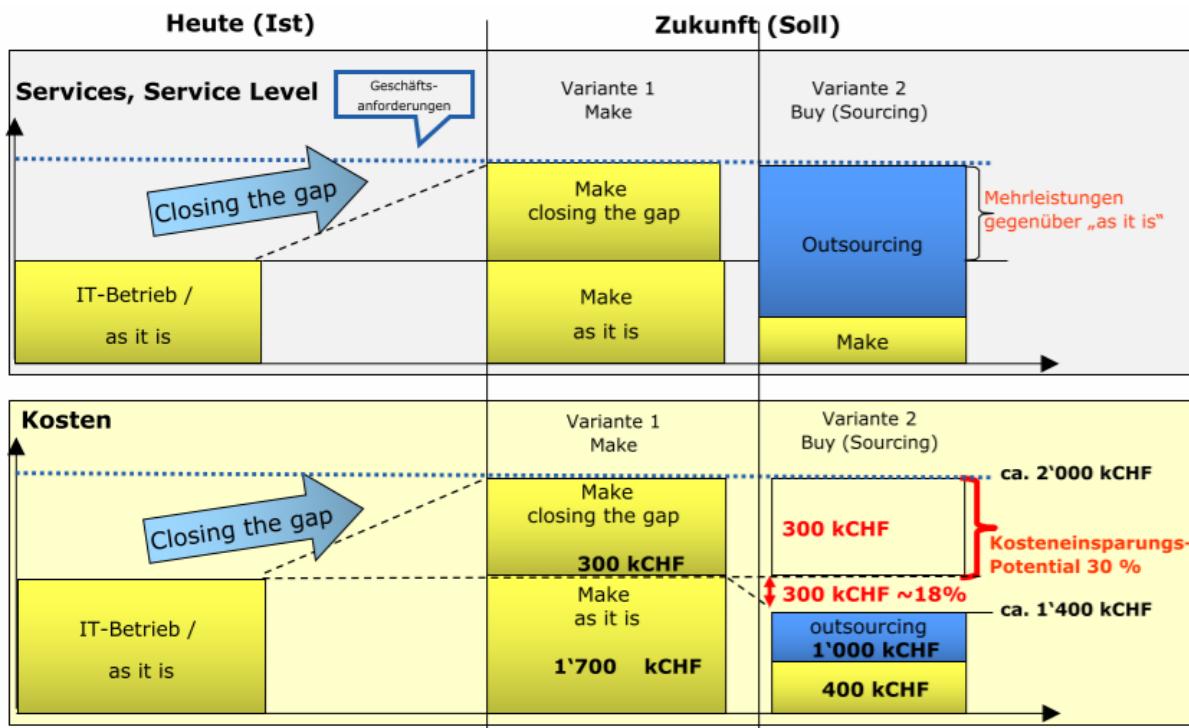
	Gruppe	Pro	Contra
Strategie	Konzentration auf das Kerngeschäft	Verlust IT-Know-how	
	Standardisierung der eingesetzten IT-Systeme	Entstehung irreversibler Abhängigkeiten	
	Reduktion des Risikos von IT-Aufgaben	Verlust Wettbewerbsrelevanz bestimmter IT-Aufgaben	
Leistung	Hohe Kompetenz des Dienstleistungsunternehmens	Unrealistische Aussagen Anbieter	
	Erhöhung der Betriebssicherheit	Unzureichende Messbarkeit Vertragserfüllung	
	Zugang fehlendes IT-Know-how	Beeinträchtigung Datenschutz	
Kosten	Kostenreduktion Betrieb	Transaktionskosten	
	Transparenz und Planbarkeit	Koordinationskosten	
	Präzisere Leistungsverrechnung	Bezugsgrößenbestimmung fehlt	
Personal	Mittelfristige Reduzierung IT-spezifische Probleme im Personalwesen	Arbeitsrechtliche Probleme Personalwiderstände	

	Job enrichment (Aufgaben) und enlargement (Verantwortung)	Motivationsprobleme
Finanzen	Glättung IT-Ausgaben	Abfindung ausscheidender Mitarbeiter
	Finanzmittelbeschaffung	Langfristig schlecht vorhersehbare Entgeltgestaltung
	Erfolgsbeteiligung von Dienstleister	Negative Auswirkungen bei wirtschaftlichen Probleme des Anbieters

5.6 Beispiel Lösungsbewertung

Vorgehen

- Make or Buy
- Bewertung qualitativer und quantitativer Aspekte
- Bewertung Nutzwertanalyse
- Entscheid für Lösung



5.7 Erfolgsfaktoren

- Strategie
- Governance
- Ausschreibungsunterlagen
- Vertrag & SLA
- Beziehungsmanagement

5.8 Outsourcing-Prozess

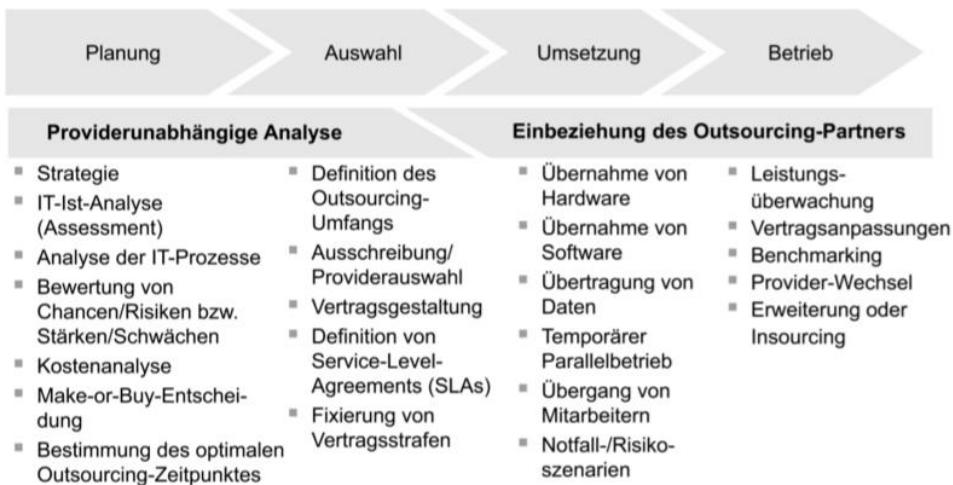


Abbildung 24: Outsourcing-Prozess

5.9 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

5.10 Chancen und Risiken IT-Outsourcing

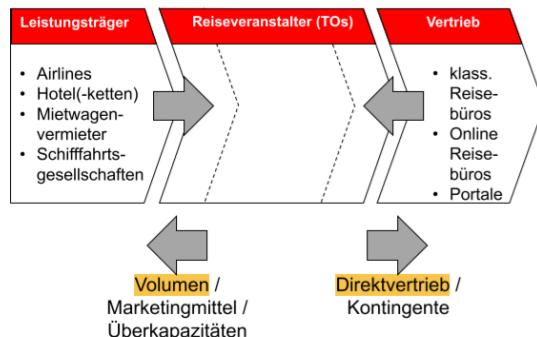
IT-Outsourcing: Chancen	IT-Outsourcing: Risiken
<ul style="list-style-type: none"> □ Kostensenkung / Fixkostenabbau □ Planbarkeit der Kosten □ bedarfsgerechte Anpassung □ Erhöhung der Flexibilität □ Vermeidung von IT Investitionen □ Abwälzung von Risiken □ erhöhte Innovationsfähigkeit □ professionelle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

6 Vali IT

6.1 Tourismus Branche im Wandel

- Entbündelung und Online Zugang
- Polarisierung (Von Normalferien zu vermehrten Billigferien)
- Überkapazitäten (Kapazitäten steigen durch Investitionen -> Kunde am längeren Hebel -> Preisdruck)

Position in der Wertschöpfungskette unter Druck



☞ Die Technologie, insbesondere die Internettechnologie, bietet in diesem Umfeld viele neuen Risiken und Chancen für alle Akteure

Lösung: Technologiegestützt Innovation für neue Geschäftsfelder.

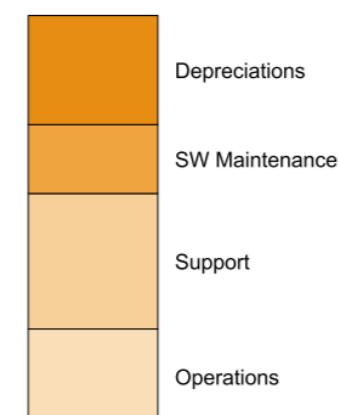
- Durch die Digitalisierung kann der Reiseveranstalter sein Angebot praktisch in Real Time verwalten. Das bedeutet, die Planungszyklen werden wesentlich kürzer. Ein Angebot wird bei der Erkennung (Anbieter) innerhalb 2 Tagen auf der Plattform (Reiseveranstalter) aufgeschaltet. Der gleiche Prozess dauerte früher 6 Monate.
- Ein weiterer Vorteil ist das Selfmanagement der Angebote durch den Anbieter. Damit ist gemeint, dass der Anbieter seine Homepage selber gestaltet und somit auch die Angebote der Reiseagenturen. Dies verringert den Aufwand des Reiseveranstalters massiv.
- Die dritte grosse Änderung wird durch die automatisierte Online Buchung ermöglicht. Dadurch können viele Prozesse welche vorher von Hand gemacht wurden automatisch erledigt werden. (z.B. Rechnungen)

6.2 Spannungsfeld zwischen Innovation und Kostendruck

Run the Business (Kostenmanagement kann in vier weitere Kategorien unterteilt werden:

Die operativen Betriebskosten (=Servicekosten) beinhalten die folgenden 4 Komponenten

- **Depreciations** (jährliche Abschreibungen aktiverer Projekte für Core und SBU spezifische Anpassungen)
- **SW Maintenance** (Bugfixing & Compliance Anpassungen für Core und SBU spezifische Anpassungen)
Sales Specific Updates
- **Support** (Businessunterstützung, Customizing, Schulung für Core und SBU spezifische Themen)
- **Operations** (incl. Data Center, Infrastruktur & Betrieb, HW-Abschreiber, Manpower (Überwachung, Betrieb, Servicedesk))



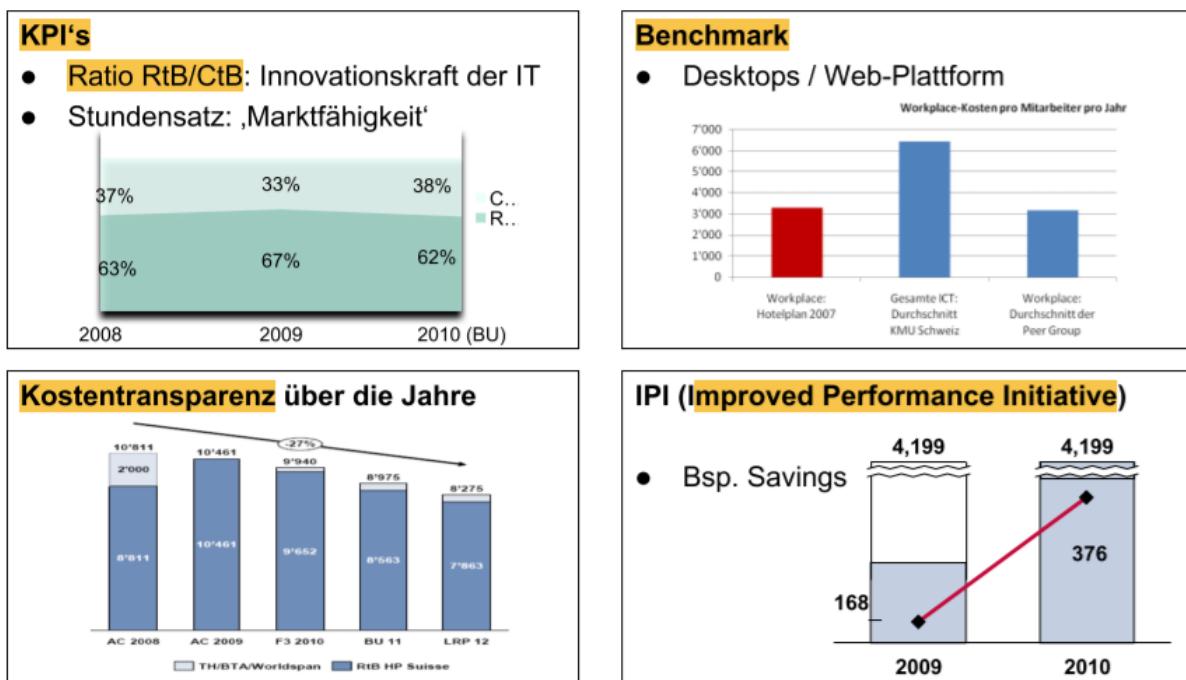


Abbildung 25: Werkzeugkasten für CIO

Zur Erkennung der Kosten können Reportings verwendet werden:

- Cost Reporting Group ICT (Wohin fliessen die Mittel?)
- Consolidated ICT Cost Reporting (Wie hoch sind die gesamten Kosten?)
- ICT BSC & Cockpit (Wie entwickeln sich unsere Kosten?)

6.3 Einführung Val IT

Ist ein Governance Framework zur Steuerung von Prozessen, Managementpraktiken, Zielen und Kennzahlen. Im Gegensatz zum klassischen Controlling fokussiert es auf Investitionen und Nutzen für den Unternehmenserfolg. Überführung von einem Assessment ermittelten IST zum SOLL Zustand.

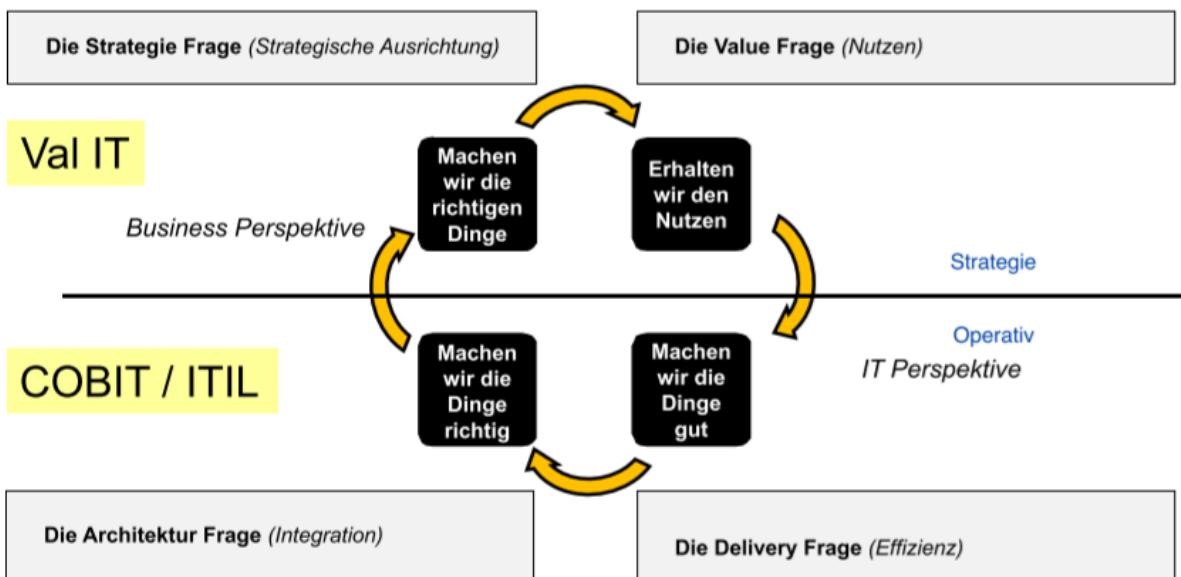


Abbildung 26: Val IT und COBIT

Val IT fokussiert sich dabei auf die Business Perspektive und somit strategische Ausrichtung. Es hat drei Domänen:

- Governance Value (Strategische Dimension)
- Portfolio Management (Taktische Dimension)
- Investment Management (Operative Dimension)

Anhand der Hotelplan ICT wurden grob folgende Schritte gemacht:

1. Identifizierter Handlungsbedarf (IST-Analyse)
 - a. Beschränktes oder fehlendes Verständnis für IT Ausgaben
 - b. Infragestellung des Nutzenbeitrags von IT
2. Ansätze aus Framework
 - a. Aufbau eines Inventars der Investitionen
 - b. Klärung des Nutzens der einzelnen Investitionen
3. Roadmap für Prozessumsetzung

6.4 Kritische Würdigung Val IT

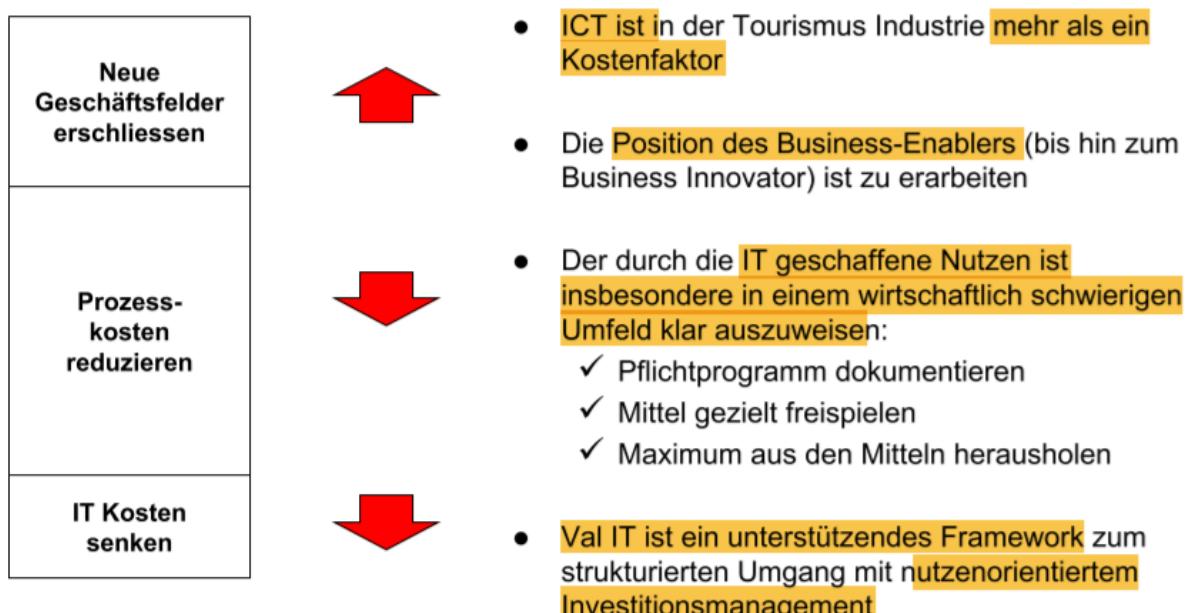
Val IT als Framework

- Relativ komplexes und mächtiges Framework (für ein mittelständisches Unternehmen)
- Leitet strukturiert an die Problematik (IST) und die Massnahmen (SOLL) heran
- „Gesunder Menschenverstand“ und „best practices“ führen zu ähnlichen Ergebnissen

Val IT beim Hotelplan

- IT-Nutzen im Tourismus ist sichtbar zu machen: Kostendruck vs. technologiegetriebene Veränderung
- Herausforderung Planungshorizont (saisonale Denke)
- Akzeptanz des Managements
- Frappante Erkenntnisse in der Retrospektive (e-Business) -> Investitionen vs. Umsatzwachstum

6.5 Zusammenfassung



7 Lizenzmanagement

Grundsätzlich soll das Lizenzmanagement helfen nicht Über- oder Unterlizenziert zu sein.

Das Lizenzmanagement beschreibt den legalen Umgang mit Software, es hat primär eine wirtschaftliche Sichtweise.

Für die technische Verwaltung wird ein Software-Asset-Management (SAM) verwendet.

Vorteile für die Implementierung eines Lizenzmanagements

- Einhaltung Volumenbeiträge
- Transparente Darstellung der Situation
- Mögliche Einsparung erkennen
- Schaffung von Compliance
- Prozesskostensenkung
- Bessere Positionierung bei Verhandlungen gegenüber Software Hersteller

7.1 Begriffsdefinitionen

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.

Lizenzmodelle beeinflussen die rechtmässige Software-Nutzung in Form folgender Faktoren:

- durch die **Lizenzart** (z. B. Einzellizenz, **Mehrplatzlizenz**)
- durch die **Lizenzkasse** (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)

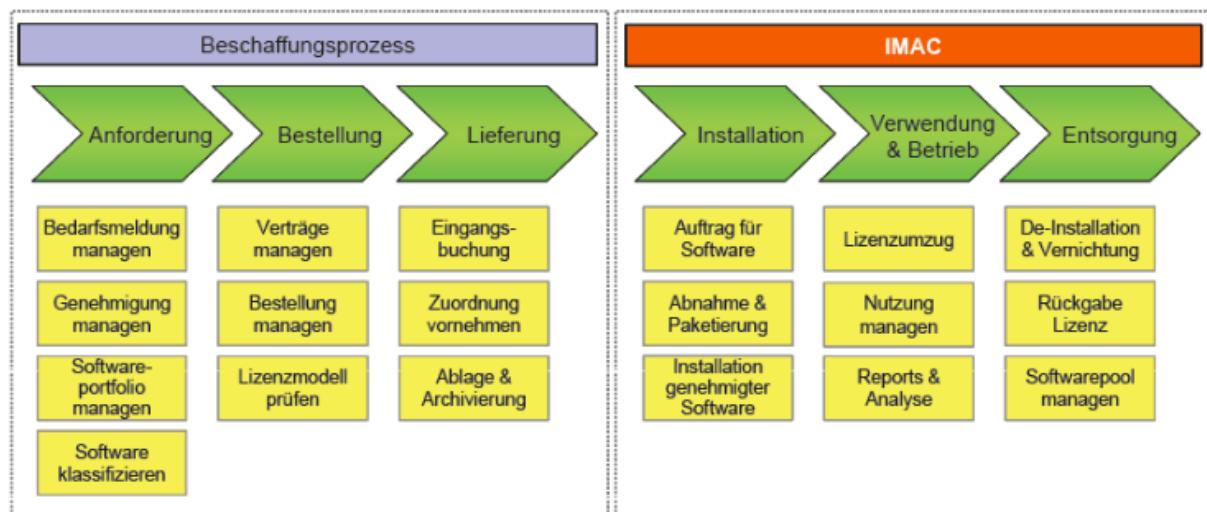
7.2 Einführung Lizenzmanagement

Nach ISO 19970-4 gibt es folgende Stufen zur Einführung:

1. Erzeugung verlässlicher Daten (Compliance Report)
2. Kontrolle des Umfelds (Definition und Abbildung von standardisierten Prozessen und Verfahren im Software Life Cycle)
3. Einbindung in die Geschäftsprozesse (Schaffung eines Single Point of Contact (SPOC))
4. Vollständige Integration (Dauerhafte operative Software-Asset- und Lizenzmanagements)

Meist macht sich ein Unternehmen erst vor dem ersten Audit Gedanken zum Lizenzmanagement, dann ist es häufig zu spät.

7.3 Software Life Cycle



7.4 Rolle Lizenzmanager

- Steuerung der Lizenzbeschaffung
- Beratung der Fachabteilung
- Definition von Richtlinien, Massnahmen und Kontrollmechanismen
- Begleiten von Software Audits
- Erstellen von Berichten und Statusreports
- Massnahmen zur Verbesserung der Lizenzmanagement Prozesse

7.5 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.

8 IT-Audit

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

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

8.1 Vorgehensmodell Anwendungsprüfung

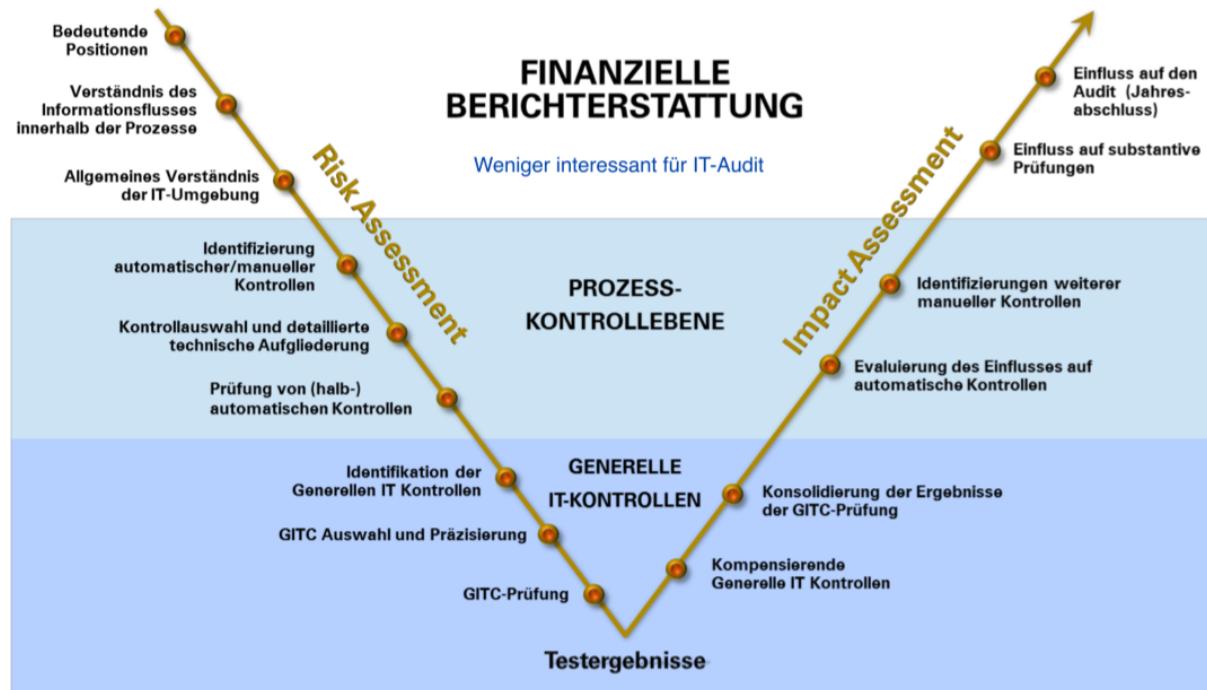


Abbildung 27: V-Modell Finanzielle Berichterstattung

8.2 Revisionsplanung

Revisionsstrategie

- Bestätigung der Jahresrechnung (Financial Statement Audit)
- Prüfung ob eine Systemmigration erfolgreich durchgeführt wurde und alle Daten vollständig und korrekt übertragen wurden (Migrationsprüfung)
- Bestätigung das bei einem Dienstleistungserbringer angemessene Kontrollen existieren (Service Provider Audit)

Ansonsten entstehen bei einem Ausfall oder Fehler in der IT signifikante Auswirkungen auf die Finanzberichterstattung, die Erfüllung regulatorischer Anforderungen oder sogar den Geschäftsfortbestand.

	Externe Revision	Interne Revision
Ziel	Effektivität	Effektivität und Effizienz
Prüftiefe	Prüfung der wesentlichsten Punkte	Oftmals Deep Dive in ein spezielles Thema
Scope	Materiell für Finanzberichterstattung	Alle Unternehmensbereiche

8.3 Prüfungsdurchführung

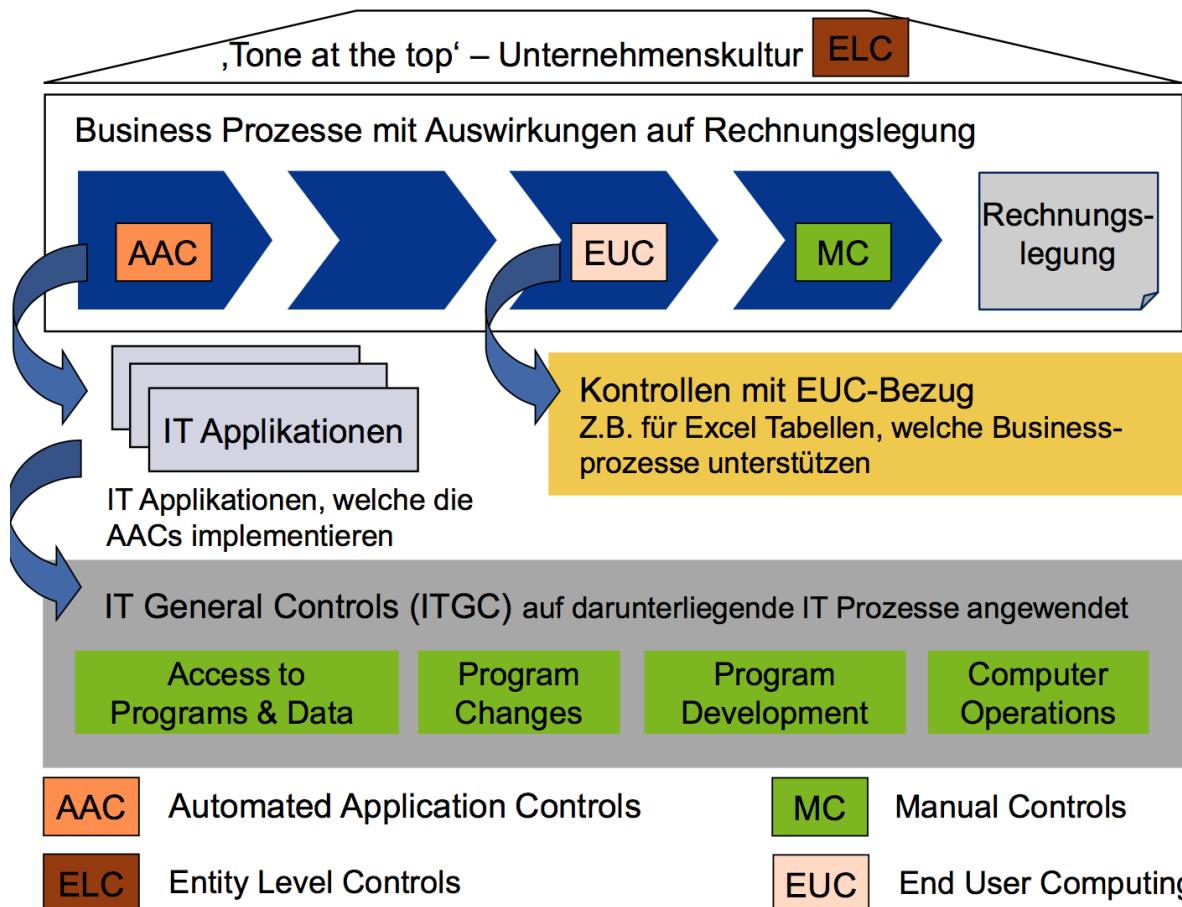


Abbildung 28: IT-Audit Kontrollarten / 4-Schichtenmodell

8.3.1 Entity Level Controls (ELC)



Sind die obersten Stufen der Kontrollen.

Die Prüfung besteht hauptsächlich aus:

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

ELC umfassen in den meisten Fällen manuelle Kontrollen. Man prüft, ob ausreichende Kontrollen über die Unternehmenskultur und Leistungserbringung bestehen. Es kommt ein Top-Down-Approach bei den Richtlinien und deren Umsetzung zum Einsatz.

8.3.2 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, Doppeleinträge	
▪ 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	

Dabei gibt es 3 Zusicherungen (Assertions) für automatisierte PLC und GITC:

- Vollständigkeit (Completeness) - Sämtliche relevante Daten wurden übertragen / verarbeitet
- Genauigkeit (Accuracy) - Daten werden verarbeitet wie eingegeben
- Existenz (Existency) - Die geprüften Dinge existieren tatsächlich

Weitere Assertions der Wirtschaftsprüfung

- Valuation (Bewertung, Wertung)
- Obligations and rights (Verpflichtung und Rechte)
- Presentation and disclosure (Einordnung und Ausweis)

8.3.3 Generelle IT Kontrollen

- Sind für alle Prozesse und Bereiche relevant
- Unterstützen das Funktionieren von PLC über die ganze Prüfperiode
- Stellen Grundsicherheit für die zu prüfende IT
- Tiefe hängt von den PLC ab

Prüfbereiche sind:

- Zugriff auf Programme und Daten (inkl. Physischer Zugang)
- Änderungswesen
- IT Entwicklung
- IT Betrieb

8.3.4 Prüfprozeduren

Folgende Prüfprozeduren können ausgeführt werden, um die Assertions abzudecken.

Prüfprozedur	Erklärung
Inspection	Betrachtung von Transaktionen, Dokumenten oder physischen Assets System Settings
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

Die Prüfungen können verfahrensorientiert oder ergebnisorientiert durchgeführt werden.

- Ergebnisorientiert: Orientierung am Resultat (konkrete Zahlen)
 - Verfahrensorientiert: Beurteilung des Prozesses (Robustheit), hier gibt es Kontrollen mit 3 Eigenschaften
 - 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: Inherent Risk of the process, without consideration of control
 - Control Risk: Risk that a material error is not detected by control

8.3.5 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!

Arten von Stichproben

- | | |
|--|--|
| ▪ Statistical Sampling | Basierend auf statistischen Methoden |
| ▪ Attribute Sampling | Vorkommen eines bestimmten Werts |
| ▪ Variable Sampling | Wertbasiert, z.B. Schätzung des Werts der Gesamtpopulation |
| Z.B. Zugriff FinSys -> Antrag mit Unterschrift | |
| ▪ Non-statistical Sampling | Basierend auf Erfahrung des Auditors |
| | Welcher Bereich hat höheres Risiko für Probleme? |

Es gibt aber auch Mischformen, z.B.

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

Wie gross müssen die Stichproben sein.

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

Automatische Kontrolle -> Sample of One. Z.B. Passwordprüfung.

Abbildung 29: Stichprobenprüfung

1+1 -> 1 aus dem ersten Halbjahr und 1 aus dem zweiten Halbjahr

8.3.6 Automatische Kontrollen

- Geringes Fehler Risiko
- Funktioniert nach der ersten korrekten Durchführung immer gleich (Test of One)
 - Solange keine Änderungen gemacht wurden
 - Die IT Kontrollen richtig funktionieren

Test of One

- Anhand einer Transaktion wird die Kontrolle nachvollzogen, wenn diese stimmt geht man davon aus, dass die anderen auch korrekt sind
- Geht nur bei gleichen Arten von Transaktionen, sonst muss für jede Art ein Test of One gemacht werden

Falls die Kontrolle seit der letzten Prüfung nicht verändert wurde und die Generelle IT Kontrollen durchgängig effektiv gemacht wurden, kann die letzten Kontrolle als Benchmarking verwendet werden.

8.3.7 Verhalten bei Exceptions

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

- Bei Automatischen Kontrollen muss der Test als nicht effektiv beurteilt werden.
- Bei Manuellen Kontrollen kann eine zweite Stichprobe genommen werden und es kann eine Toleranz angegeben werden. Anschliessen kann man durch Re-Testing oder kompensierenden Kontrollen das Problem beheben.
 - Keine Abweichungen erwartet - Test einer zweiten Stichprobe
 - Abweichung tolerierbar - Anzahl tolerierbare Fehler abhängig von Stichprobe

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

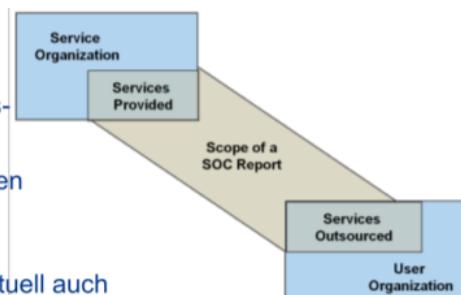
Abbildung 30: Resampling für Stichproben

8.3.8 Attestation Reports

Überprüfung der Kontrolle durch einen externen Dienstleister. Ein Attestation Report macht eine Aussage zum Design der Kontrollen (Typ 1) oder ihrer operativen Effektivität (Typ 2).

Hintergrund / Problemstellung

- Immer mehr Organisationen lagern Teile ihrer Leistungserbringung 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

8.3.9 End User-Computing (EUC)

Einsatz von IT-Mitteln (IT Applikationen) ohne Unterstützung durch generelle IT Kontrollen einer internen IT Organisation. Z.B. Applikationsfunktionalitäten in Excel oder Access.

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

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 berichtigt werden.

Kontrolle

Die End User Computing Kontrolle bezüglich der Berechnungen in dem betreffenden Excel Worksheet war nicht vorhanden. Es hatte kein sauberes Testing der Funktionalität stattgefunden.

Unternehmen setzen EUC Applikationen sehr unterschiedlich ein:

- Operationell (Überwachung und Tracking von Transaktionen, Aging Listen)
- Analytisch (Verwendung als MIS oder zur Entscheidungsunterstützung)
- Finanziell (Bestimmung von Werten, welche anschliessend verbucht werden)

Das Risiko, welches von einer EUC Applikation ausgeht, hängt stark von den durch sie wahrgenommenen Schlüsselkontrollen ab. Viele EUC Applikationen haben nur beschränkte Relevanz, da:

- Nur für die Auswertung benötigt, nicht aber für die eigentlichen Finanzzahlen, oder
- Da weitere (nicht-EUC) Schlüsselkontrollen existieren, welche besser geprüft werden können

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
 - Speicherung der Programmversionen in einem Versionierungssystems (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

8.4 IT Audit Frameworks

- ITIL ist ein Prozessframework -> Prozesslastig
- Cobit ist ein Kontrollframework -> Kontrolllastig

8.4.1 ISACA

Information Systems Audit and Control Association

- Globale Organisation der IT Revisoren und verwandten Funktionen
- Bieten verschiedene Zertifizierungen an
- Verwaltet verschiedene Hilfsmittel und Standards zur Durchführung von IT Audits
- Standards sind für Mitglieder verbindlich
- Publiziert COBIT Framework

8.4.2 COBIT

Control Objectives for Information and Related Technology

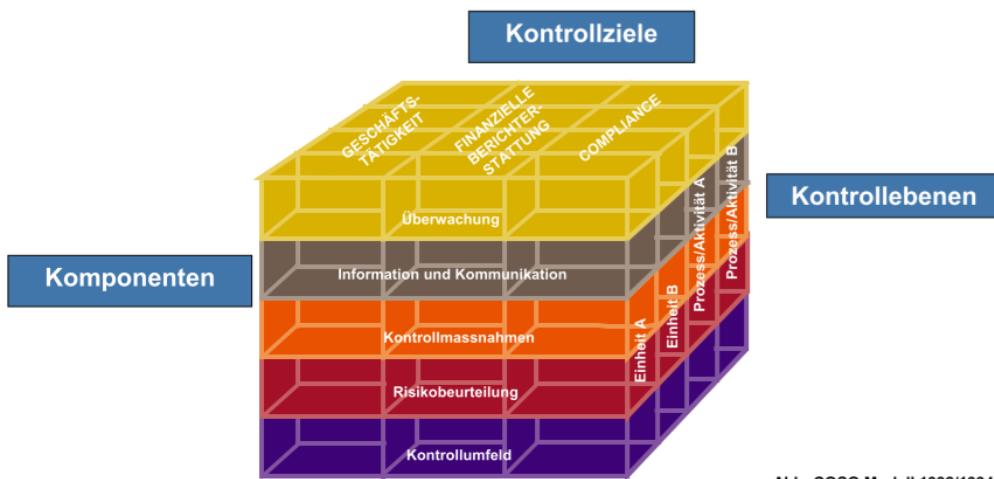
- Entwickelt von ISACA
- Umfassendes IT Governance und Management Framework
- Kontinuierlich weiterentwickelt von Bottom-Up Ansatz zu heitiger Version, welche auch von Unternehmenszielen aus Top-Down verwendet werden kann
- Beinhaltet in der neusten Version auch Risk Management und Value Management

RACI

- Responsible - Operative Verantwortung
- Accountable - Ultimative Verantwortung
- Consulted - Konsultiert
- Informed - Informiert

8.4.3 COSO

- Committee of Sponsoring Organizations of the Treadway Commission
- Zielsetzung: Förderung der qualitativen Verbesserung der Finanzberichterstattungen durch ethisches Handeln, wirksame interne Kontrollen und gute Unternehmensführung



8.5 Ergebnisbewertung

8.5.1 Dokumentation

- Dokumentation muss einen fachkundigen Dritten erlauben, die durchgeführten Prüfaktivitäten, die getroffenen Annahmen sowie die gezogenen Schlüsse nachzuvollziehen
- Immer mehr Prüfungsgesellschaften unterstützen die Dokumentation mit Workflow-Tools und Dokument-Repositorien
 - Zentrale Speicherung von relevanten Unterlagen
 - Erzwungene Einhaltung von Methodologie und Konsistenz der Dokumentation
 - Ev. Vollständig elektronische Archivierung
 - Nachteile: Restriktionen bezüglich Verfügbarkeit / Verlust an Flexibilität
- Arbeitspapier enthält folgendes:
- Ziele
 - Durchgeführte Prüfungshandlungen
 - Schlussfolgerung
 - Detaillierte Beschreibung Prüfungshandlungen
 - Prozessbeschrieb
 - Prüfung Design Effectiveness (ToD)
 - Prüfung Operating Effectiveness (ToE)
 - Evidenzliste

8.5.2 Bewertung

Prüfungsergebnisse mit möglichem Einfluss auf die Beurteilung:

- **Kontrolle ist in ihrem Design nicht geeignet, die Kontrollzielen 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 können

Vorgehen im Fall einer einzelnen ineffektiven Applikationskontrolle:

- Beurteilung der Behebung der Kontrollschwächen
- 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 Kontrollschwächen zu bestimmen

Fragen im Fall, dass eine Applikationskontrolle ein Kontrollziel nicht erreicht:

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

Wenn bei allen Fragen Nein, so wird der Prüfungsansatz für das entsprechende Prüfziel verändert -> Ergebnisorientierten Prüfansatz (Zusatzaufwand für Aufsetzen neue Prüfung / Massiv höherer Aufwand für die Prüfung)

8.5.3 Ineffektive Generelle IT Kontrollen (Gesamthaft)

Werden die GITC für eine bestimmte Applikation als gesamthaft nicht effektiv beurteilt so hat dies folgende Auswirkungen:

- Auch wenn die unterstützende 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 dies Ausführung geprüft werden, um angemessene Sicherheit über das Funktionieren der Applikationskontrolle zu erhalten
- Bsp. 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 -> Vorgehen bei ineffektiven Applikationskontrollen zur Anwendung.

8.5.4 Inneffektive Generelle IT-Kontrolle (Einzeln)

Wird eine einzelne GITC 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 durchgeführten (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.

8.6 Herleitung Massnahme

Beispiel einer Herleitung:

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** daran **gemessen**, dass sie **keine Feststellungen von der externen und internen Revision** haben
- Mehrere Managementstufen nacheinander ihr Einverständnis geben
- Feststellungen immer faktisch korrekt und neutral formulieren
- **Stellungnahme des Verantwortlichen**
 - Akzeptanz der Feststellung
 - Kurzbeschreibung der geplanten Gegenmassnahmen
 - Fristansetzung für die Gegenmassnahmen

Jede Feststellung sollte früher oder später auf ihre **Behebung hin überprüft** werden

- Externe Revision (Scope jedes Jahr gleich / Rollende Planung)
 - Auf Ende des Geschäftsjahres (falls Behebung sofort erfolgt)
 - Im nächsten Geschäftsjahr

- Interne Revision
 - In der Regel im Rahmen der **nächsten Überprüfung**
 - Bei schweren Feststellungen werden diese oft zu Veränderungen in der Prüfungsplanung führen, so dass eine Prüfung im nächsten Geschäftsjahr ansteht
- Nichteinhaltung der Umsetzung / Termine wird von vielen Unternehmen intern massiv bestraft
- Unterscheidung mit Repeat Issues, welche noch nicht behoben werden mussten

8.7 Vorgehensmodell

Ziel: Testierung der finanziellen Rechnung.

8 Schritte des Modells:

1. Analyse von Bilanz und Erfolgsrechnung
2. Identifikation der Geschäftsprozesse und Datenflüsse
3. Identifikation der Kernanwendungen und der IT-relevanten Schnittstellen
4. Identifikation der Risiken und Schlüsselkontrollen
5. Walk-Through
6. Beurteilung des Kontroll-Designs
7. Beurteilung der Umsetzung der Kontrollen
8. Gesamtbeachtung und Ergebnisfindung

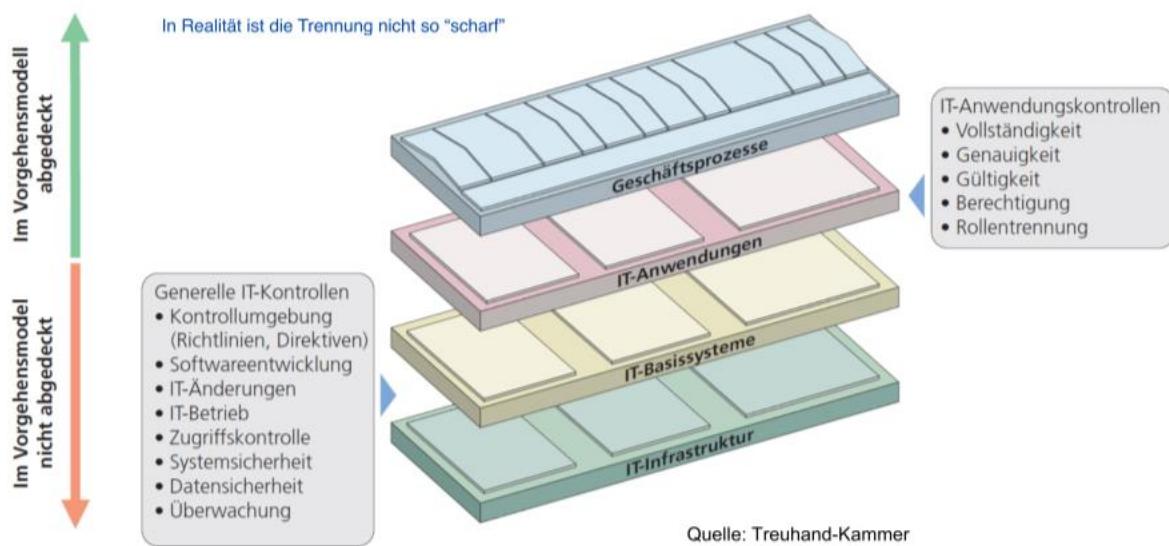


Abbildung 31: IT-Audit Vorgehensmodell

9 Verzeichnisse

9.1 Abbildungsverzeichnis

Abbildung 1: COBIT 5 Anspruchsgruppen	2
Abbildung 2: COBIT 5 Enabler	3
Abbildung 3: COBIT 5 Kernbereich von Governance und Management	3
Abbildung 4: Wertbeitrag der IT	4
Abbildung 5: Elemente IT-Kostenmanagement	5
Abbildung 6: Chancen- und Risiko-Portfolio	5
Abbildung 7: Porter Kräftemodell	7
Abbildung 8: Ansatzpunkte für die Digitalisierung	7
Abbildung 9: Auswirkungen der Digitalisierung auf die Geschäftswelt	8
Abbildung 10: Auswirkungen der digitalen Transformation	8
Abbildung 11: Beispiele für die drei Dimensionen	9
Abbildung 12: Referenzmodell digitale Transformation	9
Abbildung 13: Stakeholder Business Case	11
Abbildung 14: Bausteine Business Case	11
Abbildung 15: 3 Phasen der BC-Erstellung	12
Abbildung 16: BC Vorgehensmodell	12
Abbildung 17: Festlegung des Nutzens	12
Abbildung 18: BC Nutzenkategorien	13
Abbildung 19: Social Media ROI	14
Abbildung 20: Outsourcing Scope und Formen	15
Abbildung 21: Outsourcing-Bewertung - Unternehmenseffizient und Wertschöpfung	16
Abbildung 22: Outsourcing-Bewertung - Strategische Relevanz und Auslagerungsbarrieren	16
Abbildung 23: Sourcing Dimensionen	17
Abbildung 24: Outsourcing-Prozess	19
Abbildung 25: Werkzeugkasten für CIO	21
Abbildung 26: Val IT und COBIT	21
Abbildung 27: V-Modell Finanzielle Berichterstattung	25
Abbildung 28: IT-Audit Kontrollarten / 4-Schichtenmodell	26
Abbildung 29: Stichprobenprüfung	29
Abbildung 30: Resampling für Stichproben	30
Abbildung 31: IT-Audit Vorgehensmodell	35

9.2 Begriffsverzeichnis

Begriff	Erklärung
Governance	Governance stellt sicher, dass die Anforderungen, Rahmenbedingungen und Möglichkeiten der Anspruchsgruppen evaluiert werden, um ausgewogene und vereinbarte Unternehmensziele zu bestimmen, die es zu erreichen gilt. Sie gibt die Richtung durch die Festlegung von Prioritäten und das Fällen von Entscheidungen vor und überwacht die Leistung und Regeleinhaltung gegen vereinbarte Vorgaben und Ziele. Zuständigkeit: Geschäftsleitung
Compliance	Funktion im Unternehmen, die für die Sicherstellung der Einhaltung von rechtlichen, behördlichen und vertraglichen Anforderungen zuständig ist.
Management (Exekutive = Ausführend)	Management plant, erstellt, betreibt und überwacht Aktivitäten im Rahmen der von der Governance vorgegebenen Richtung, um die Unternehmensziele zu erreichen. Umsetzen der IT-Governance und Aufbau des IT-Controlling (Planen, Steuern, Informationsbereitstellung) Zuständigkeit: Geschäftsführung (CEO)
Produktivitätsparadoxon	Insbesondere im Dienstleistungssektor, kein positiver Zusammenhang zwischen Investitionen in die IT und der Produktivität auf volkswirtschaftlicher oder unternehmerischer Ebene zu bestehen scheint. Gründe sind: <ul style="list-style-type: none"> • Unzureichende Nutzung der Potentiale • Verzögerung zwischen IT-Einsatz und Wirkung