Zusammenfassung

IT Audit

WIIMR06

Samstag, 26. November 2016

*Autor:*

Severin Jörg

**Inhalt**

[1 Dario Gugolz 5](#_Toc485801695)

[1.1 Begrifflichkeiten 5](#_Toc485801696)

[1.2 COBIT 5 5](#_Toc485801697)

[1.2.1 Prinzip 1: Erfüllung der Anforderungen der Anspruchsgruppen 5](#_Toc485801698)

[1.2.2 Prinzip 2: Abdeckung des gesamten Unternehmens 6](#_Toc485801699)

[1.2.3 Prinzip 3: Anwendung eines einheitlichen, integrierten Rahmenwerks 6](#_Toc485801700)

[1.2.4 Prinzip 4: Ermöglichung eines ganzheitlichen Ansatzes 6](#_Toc485801701)

[1.2.5 Prinzip 5: Unterscheidung zwischen Governance und Management 6](#_Toc485801702)

[2 Guido Kaufmann 7](#_Toc485801703)

[2.1 Wertbeitrag der IT 7](#_Toc485801704)

[2.1.1 Grundlegende Unterscheidung der IT Strategie 7](#_Toc485801705)

[2.1.2 Einfluss der IT auf Umsatz und Kosten 7](#_Toc485801706)

[2.1.3 Elemente des IT-Kostenmanagements 7](#_Toc485801707)

[2.1.4 Prozessanalyse 8](#_Toc485801708)

[2.1.5 Portfolioanalyse 8](#_Toc485801709)

[2.2 Digital Business 9](#_Toc485801710)

[2.2.1 Digitalisierung 9](#_Toc485801711)

[2.2.2 5-Kräfte-Modell und digitale Transformation (Porter) 9](#_Toc485801712)

[2.2.3 Ansatzpunkte für die Digitalisierung 10](#_Toc485801713)

[2.2.4 Veränderung der Geschäftswelt durch die digitale Revolution 10](#_Toc485801714)

[2.2.5 Transformation in drei Dimensionen 11](#_Toc485801715)

[2.2.6 Referenzmodell Digitalisierung 11](#_Toc485801716)

[2.2.7 Schritte zum digitalen Wandel 11](#_Toc485801717)

[2.2.8 Kritik und Ausblick 12](#_Toc485801718)

[2.2.9 Handlungsempfehlungen im Umgang mit Digitalisierung 12](#_Toc485801719)

[2.3 Business Case und Wirtschaftlichkeitsanalyse 12](#_Toc485801720)

[2.3.1 Bausteine (Elemente) eines Business Cases 12](#_Toc485801721)

[2.3.2 Arten von Business Cases 13](#_Toc485801722)

[2.3.3 Business Case Erstellung 13](#_Toc485801723)

[2.3.4 Nutzenkategorien 13](#_Toc485801724)

[2.3.5 Business Case für Social Media (Kunden-Community) 14](#_Toc485801725)

[2.3.6 Finanzielle Kennzahlen 14](#_Toc485801726)

[2.4 Outsourcing 15](#_Toc485801727)

[2.4.1 Formen des Outsourcings 15](#_Toc485801728)

[2.4.2 Bewertung für mögliche Outsourcing-Kandidaten 15](#_Toc485801729)

[2.4.3 Prinzipien 16](#_Toc485801730)

[2.4.4 Argumentenbilanz zum Outsourcing 16](#_Toc485801731)

[2.4.5 Erfolgsfaktoren von Sourcing 17](#_Toc485801732)

[2.4.6 Chancen und Risiken 17](#_Toc485801733)

[2.5 Hotelplan 18](#_Toc485801734)

[2.5.1 IT als Business Enabler 18](#_Toc485801735)

[2.5.2 Spannungsfeld zwischen Innovation und Kostendruck 18](#_Toc485801736)

[2.5.3 Val IT 18](#_Toc485801737)

[2.5.4 Zusammenfassung 19](#_Toc485801738)

[2.6 Lizenzmanagement 19](#_Toc485801739)

[2.6.1 Nutzen 19](#_Toc485801740)

[2.6.2 Reifegradmodell 20](#_Toc485801741)

[2.6.3 Software Life Cycle 20](#_Toc485801742)

[2.6.4 Lizenzmanager 20](#_Toc485801743)

[3 Max Zeilinger 21](#_Toc485801744)

[3.1 Planung 21](#_Toc485801745)

[3.1.1 Prüfungsstandard 200 21](#_Toc485801746)

[3.1.2 Prüfungsstandard 400 21](#_Toc485801747)

[3.1.3 Prüfungsstandard 401 (Umfeld der IT) 21](#_Toc485801748)

[3.1.4 Revisionsstrategie 21](#_Toc485801749)

[3.1.5 Prüfungsorganisation 22](#_Toc485801750)

[3.2 Prüfungsdurchführung 23](#_Toc485801751)

[3.2.1 Entity Level Controls (ELC) 23](#_Toc485801752)

[3.2.2 Process Level Controls 24](#_Toc485801753)

[3.2.3 Generelle IT Kontrollen 24](#_Toc485801754)

[3.2.4 Prüfprozeduren 24](#_Toc485801755)

[3.2.5 Manuelle Kontrollen 25](#_Toc485801756)

[3.2.6 Automatische Kontrollen 25](#_Toc485801757)

[3.2.7 Verhalten bei Exceptions 26](#_Toc485801758)

[3.2.8 Attestation Reports 26](#_Toc485801759)

[3.2.9 End User Computing (EUC) 26](#_Toc485801760)

[3.3 Frameworks 27](#_Toc485801761)

[3.3.1 ISACA 27](#_Toc485801762)

[3.3.2 COBIT 27](#_Toc485801763)

[3.4 Dokumentation 28](#_Toc485801764)

[3.5 Bewertung Ergebnisse 28](#_Toc485801765)

[3.5.1 Einzelne ineffektive Applikationskontrolle 28](#_Toc485801766)

[3.5.2 Inneffektive Generelle IT Kontrollen (Gesamthaft) 29](#_Toc485801767)

[3.5.3 Ineffektive Generelle IT Kontrolle (Einzel) 29](#_Toc485801768)

[3.6 Herleitung Massnahmen 29](#_Toc485801769)

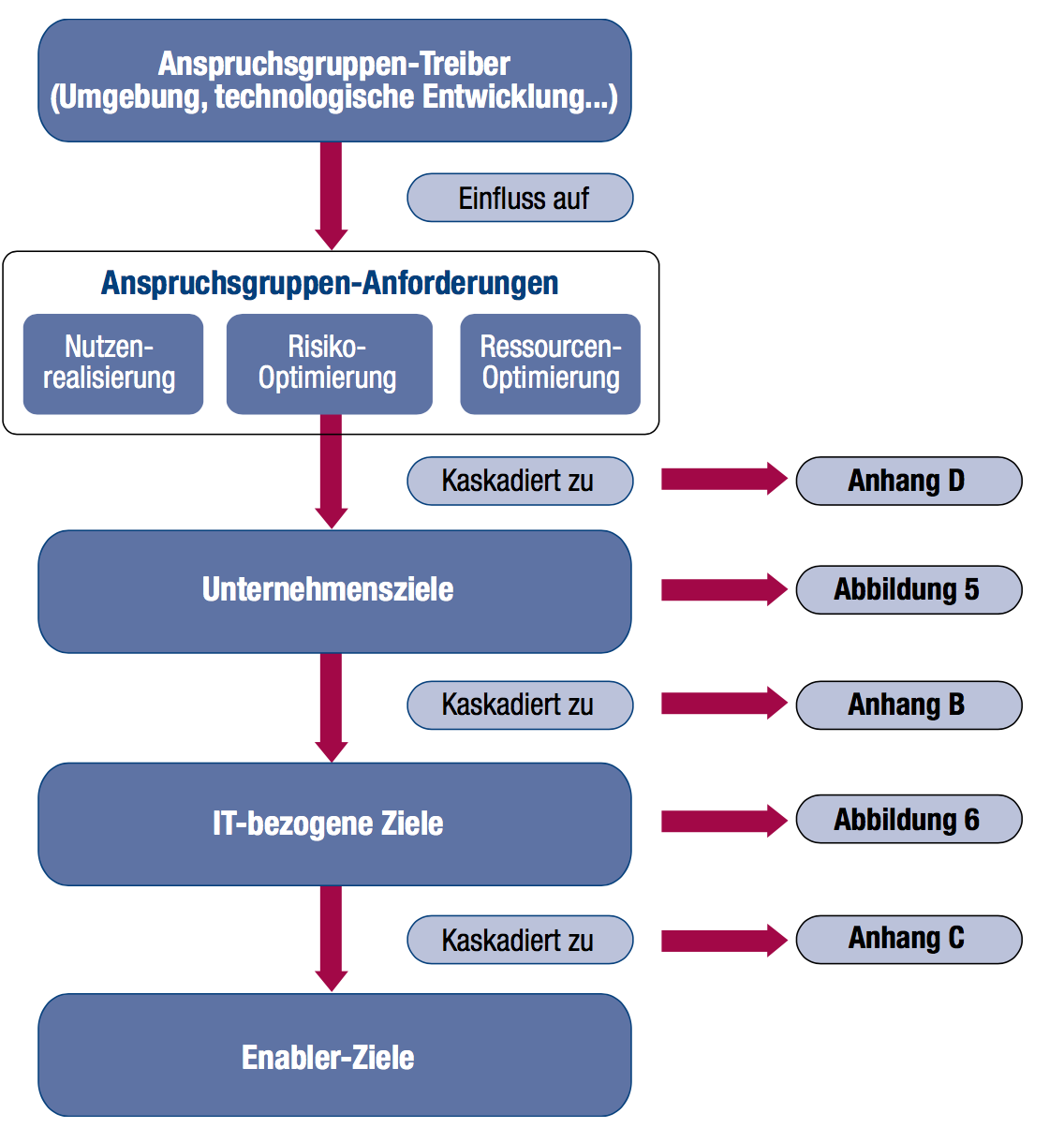
[3.7 Vorgehensmodell der Schweizer Treuhand-Kammer 30](#_Toc485801770)

# Dario Gugolz

## Begrifflichkeiten

|  |  |
| --- | --- |
| Governance (Legislative = Gesetzgebend) | 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 |
| IT Governance | Betrifft die Organisation, Steuerung und Kontrolle der IT eines Unternehmens zu konsequenten Ausrichtung der IT-Prozesse an der Unternehmensstrategie. |
| 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) |
| Vom Groben ins Feine | * Policies („Wir schützen unsere Devices) * Standards (Technologie- oder Produktvorgaben) * Guidelines (Tipps & Tricks) * Procedures (vorgegebene Workflows, Checklisten) |
| Ziele IT Governance | * Strategische Ausrichtung mit Fokus auf Unternehmenslösung * Nutzengenerierung mit Fokus auf die Optimierung der Ausgaben und Bewertung des Nutzens der IT * Risikomanagement (Disaster Recovery & Business Continuity Management) * Management von Ressourcen, Optimierung von Wissen und Infrastruktur |

## 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.

### 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.

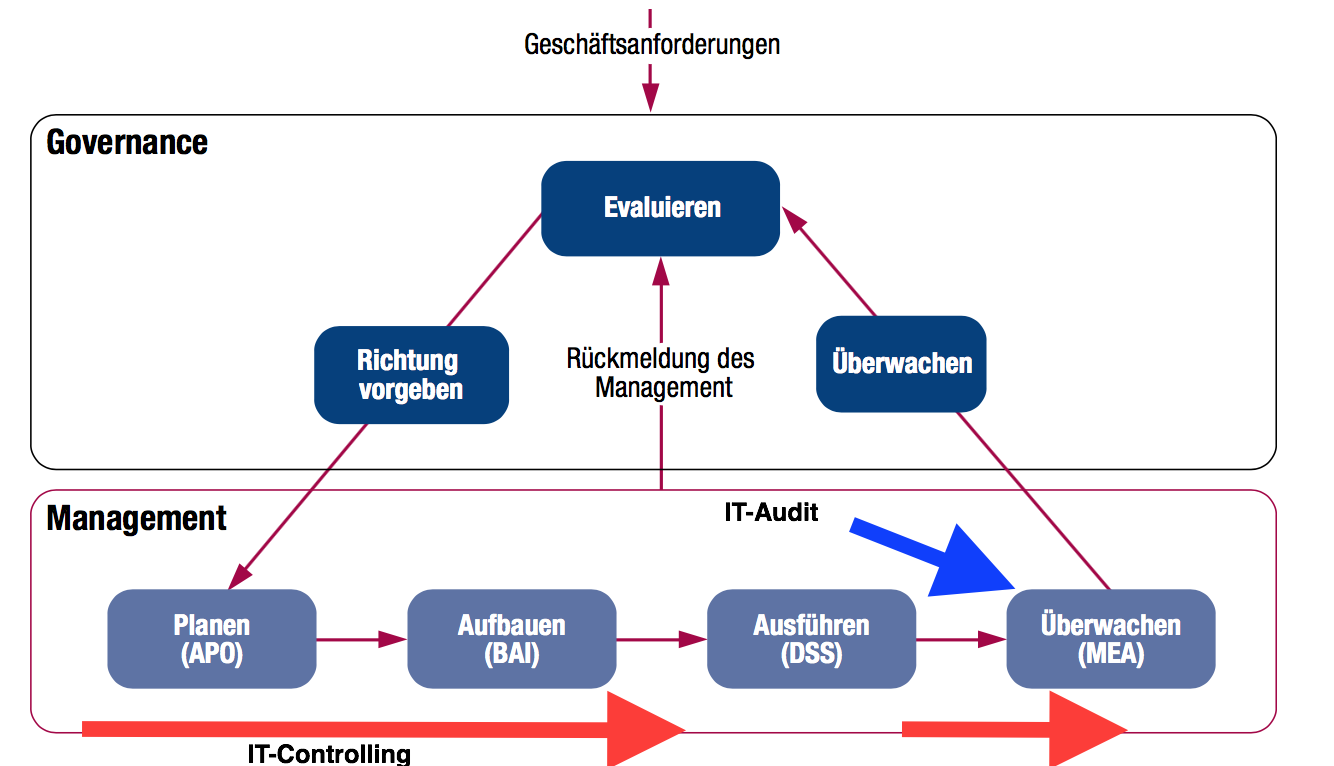
### Prinzip 3: Anwendung eines einheitlichen, integrierten Rahmenwerks

* 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.

### 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.

|  |  |  |
| --- | --- | --- |
| 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 |

# Guido Kaufmann

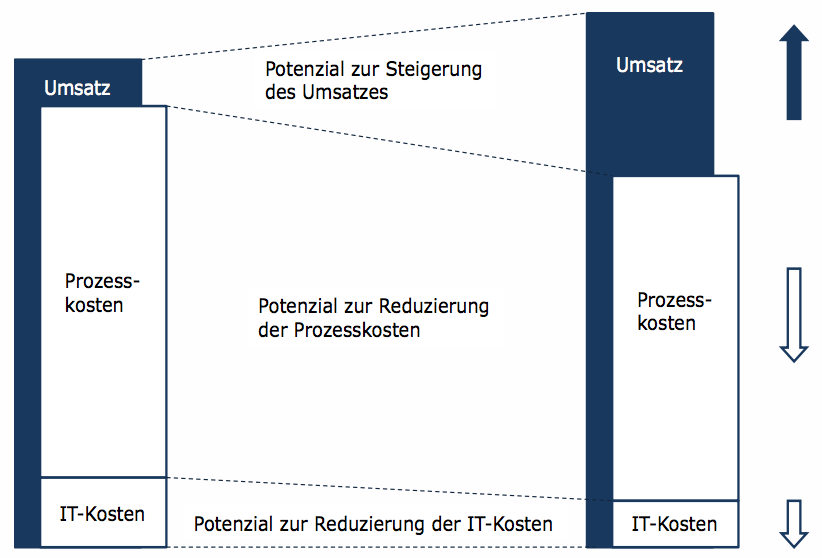
## Wertbeitrag der IT

### Grundlegende Unterscheidung der IT Strategie

* **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.

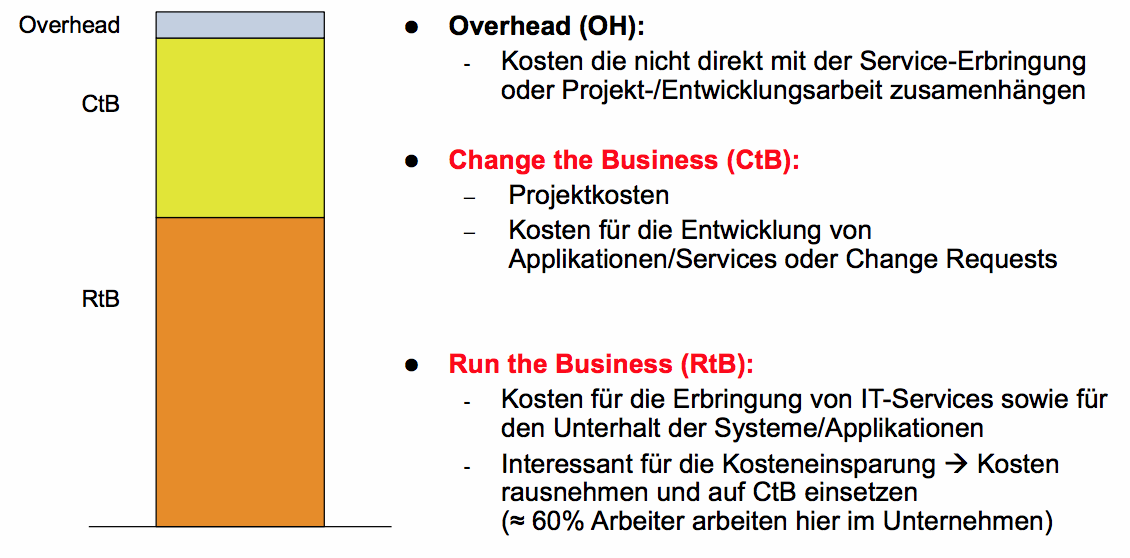
|  |  |
| --- | --- |
| Produktivitäts-paradoxon | Insbesondere im Dienstleistungssektor, kein positiver Zusammenhang zwischen Investitionen in die IT und der Produktivität auf volkswirtschaftlicher oder unternehmerischer Ebene zu bestehen scheint. Gründe sind:   * Unzureichende Nutzung der Potentiale * Verzögerung zwischen IT-Einsatz und Wirkung |

### 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 Kundenzufriedenheit aus. Neben den Kosten ist zwingend das Potential auf den Umsatz zu analysieren.

* Umsatzsteigerung: Neue Geschäftsfelder erschliessen
* Prozesskostenreduktion: Prozessoptimierung und –automatisierung
* IT-Kostenreduktion: Günstige Lizenzen, Systeme abstellen

### Elemente des IT-Kostenmanagements

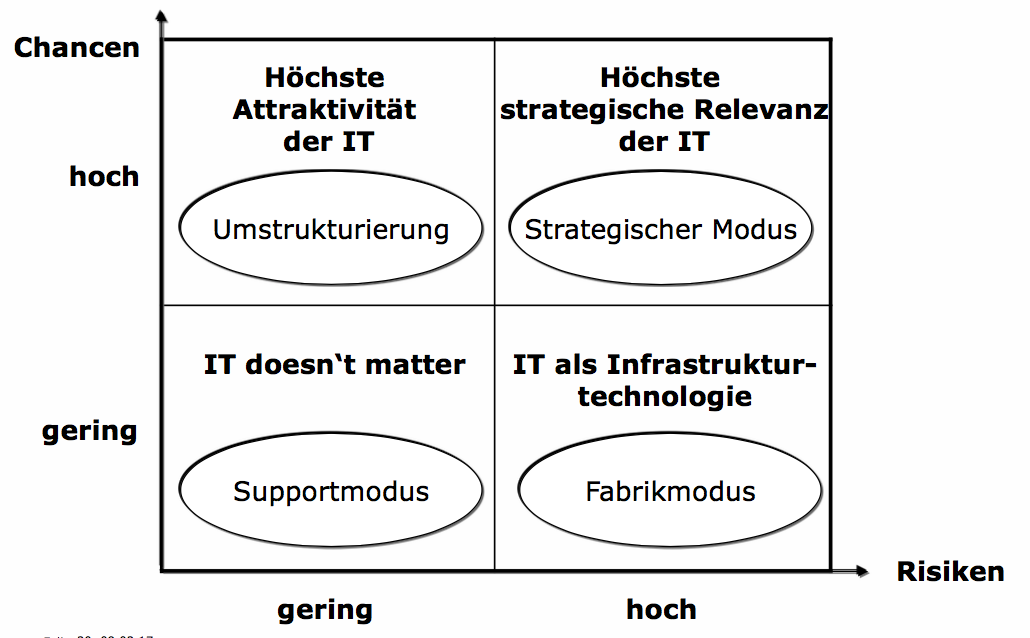


### Prozessanalyse

Die IT kann bei klassischen Prozessen wie beim Buchungsprozess vorwiegend zur Effizienz-Steigerung durch Digitalisierung beitragen. Um dies zu erreichen wird eine Ist-Analyse gemacht.

1. Im ersten Schritt werden die Prozesse in Teilprozesse und Aktivitäten unterteilt
2. Für die einzelnen Teilprozesse oder Aktivitäten werden einzeln die Zeitaufwände ermittelt und in den Gesamtkontext gestellt (% der Gesamtzeit)
3. Zudem werden die Materialaufwände (Sachkosten) ermittelt
4. Die Sach- und Personalkosten ergeben die Prozesskosten

### Portfolioanalyse



#### 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

## Digital Business

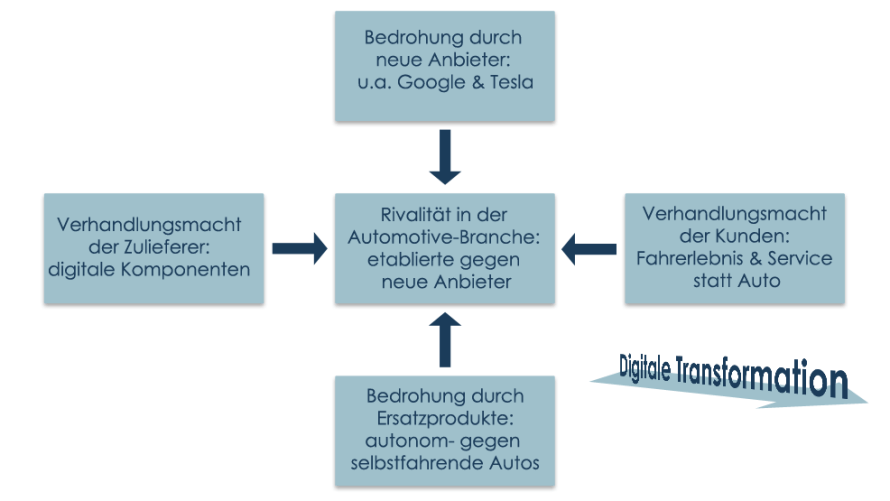
### Digitalisierung

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

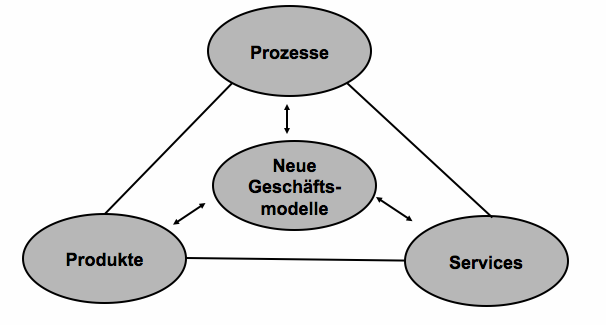
|  |  |
| --- | --- |
| Industrie 1.0 | Mensch |
| Industrie 2.0 | Elektrizität |
| Industrie 3.0 | Computer |
| Industrie 4.0 | Digitalisierung |

### 5-Kräfte-Modell und digitale Transformation (Porter)

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.



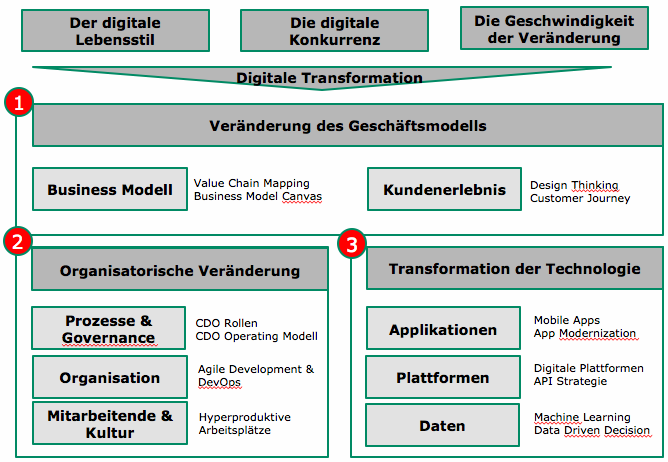
### Ansatzpunkte für die Digitalisierung



### Veränderung der Geschäftswelt durch die digitale Revolution

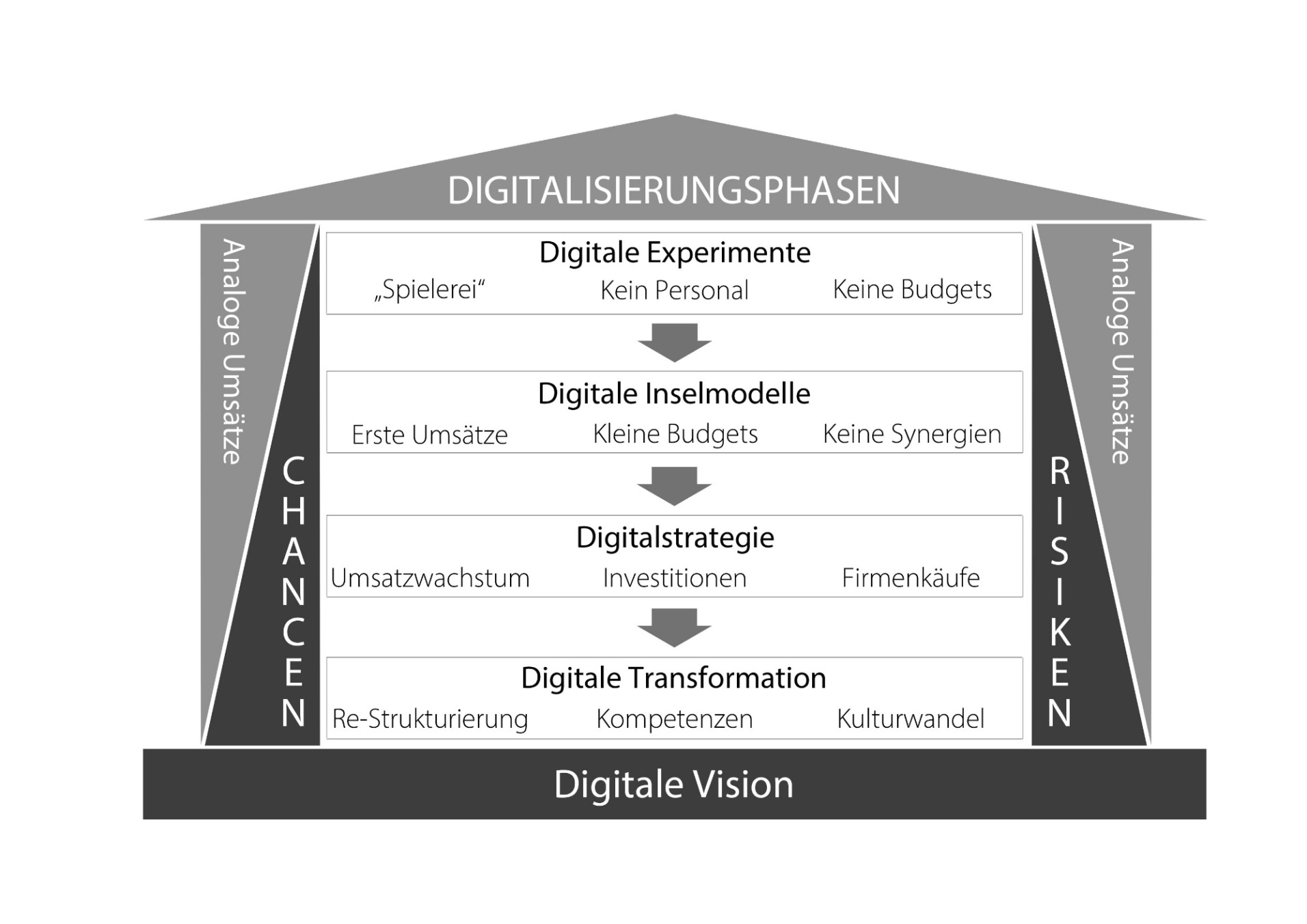


### Transformation in drei Dimensionen



* **Veränderung des Geschäftsmodells**: „Wie werden wir Teil des digitalen Lebensstils unserer Kunden?“
* **Organisatorische Veränderung**: „Ist unsere Organisation bereit, externe / interne Innovation zu implementieren?“
* **Transformation der Technologie**: „Wie muss sich unsere Technologielandschaft entwickeln?

### Referenzmodell Digitalisierung



### Schritte zum digitalen Wandel

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

### Kritik und Ausblick

* Technik- und Informationsethik: Verlust der persönlichen und informationellen Autonomie
* Wirtschaftsethik: Verantwortung der Unternehmen bei der Datennutzung und bei Fertigungsprozessen gegenüber Benutzer und Mitarbeitern
* Durch Automatisierung vermehrte Einsparung von Stellen möglich.

### Handlungsempfehlungen im Umgang mit Digitalisierung

* Technologie als Chance
* Neue Strategien
* Digitalisierung vom Kunden herdenken (Customer Journey)
* Rollen im Unternehmen neu definieren

## Business Case und Wirtschaftlichkeitsanalyse

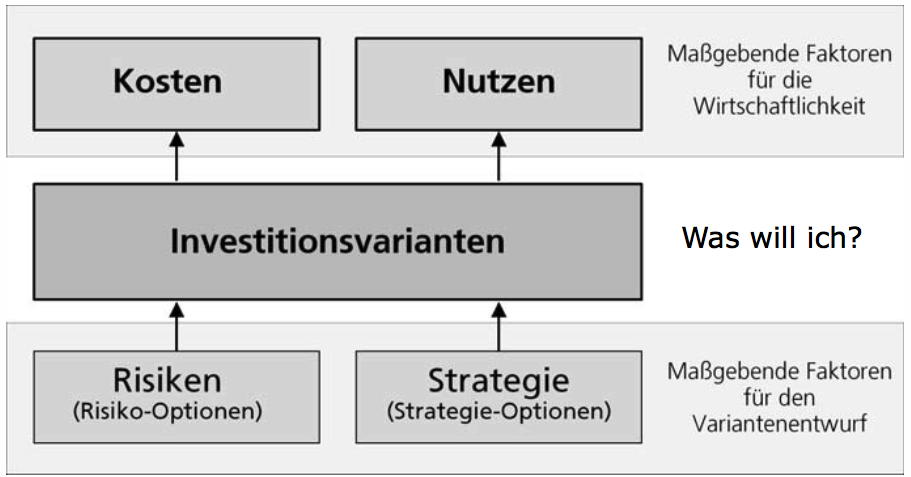
Ein Business Case fasst alle entscheidungsrelevanten Aspekte eines geplanten Vorhabens (Geschäftsszenarios) mit dem Ziel zusammen, die **wirtschaftliche Vorteilhaftigkeit** und **strategische Konformität** des Gesamtprojekts aufzuzeigen und eine abschliessende Management Entscheidung über dessen Ausführung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

Beim Business Case gibt es 4 Stakeholder:

* IT
* Business Unit
* Finanzabteilung / Controlling
* Personalabteilung

### Bausteine (Elemente) eines Business Cases

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.

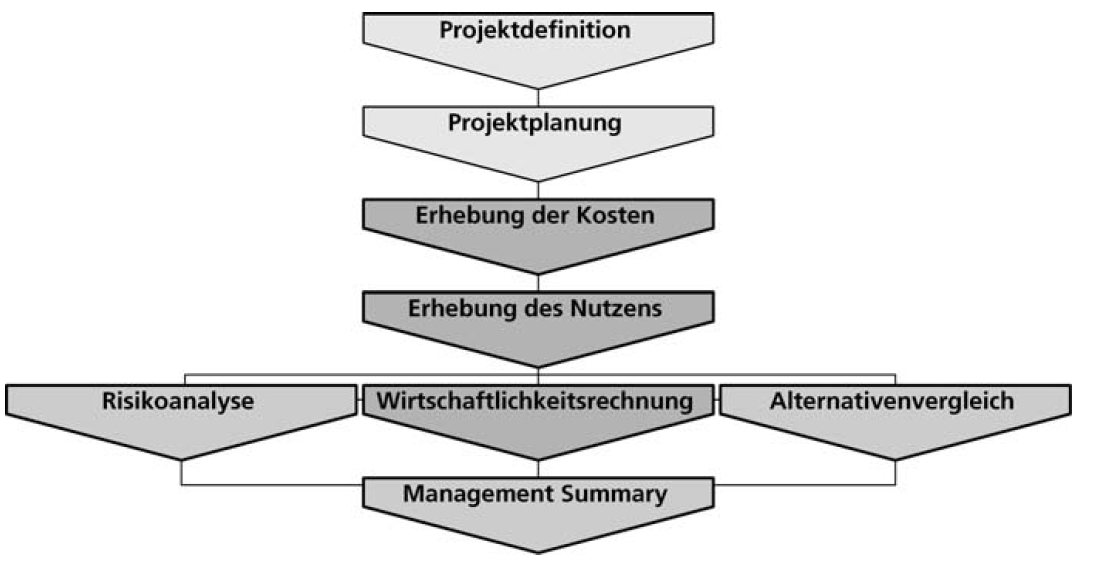


### Arten von Business Cases

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 (Ja/Nein)?
* **Auswahlentscheidung – Relative Vorteilhaftigkeit**: Welche Investitionsalternative ist vorteilhafter?

### Business Case Erstellung

Ein Business Case wird in drei Phasen (Initialisierung, Entwicklung, Prüfung) durchgeführt.

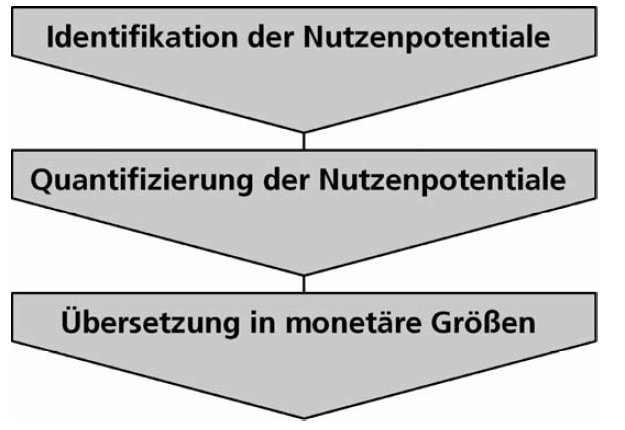
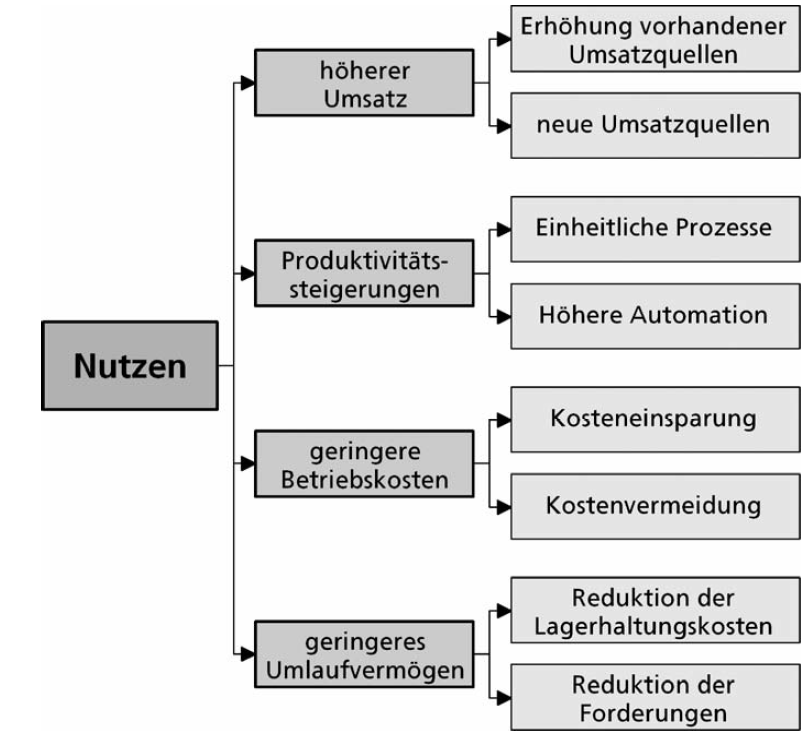
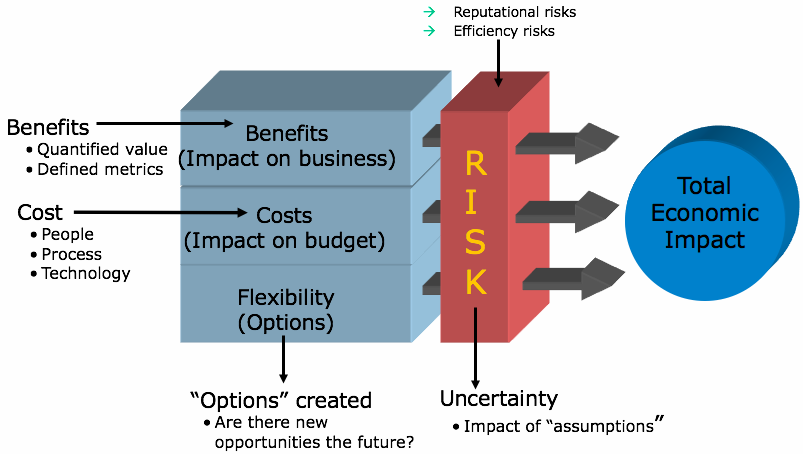


Abbildung Festlegung des Nutzens

### Nutzenkategorien



### Business Case für Social Media (Kunden-Community)



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.

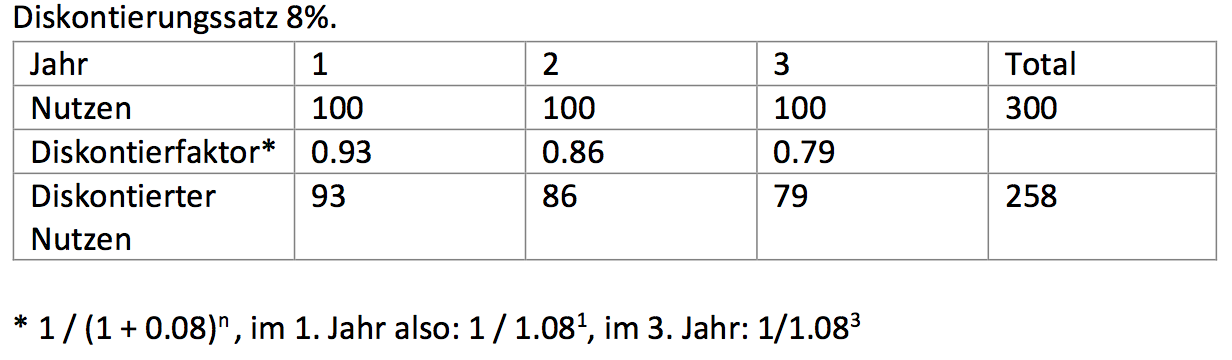
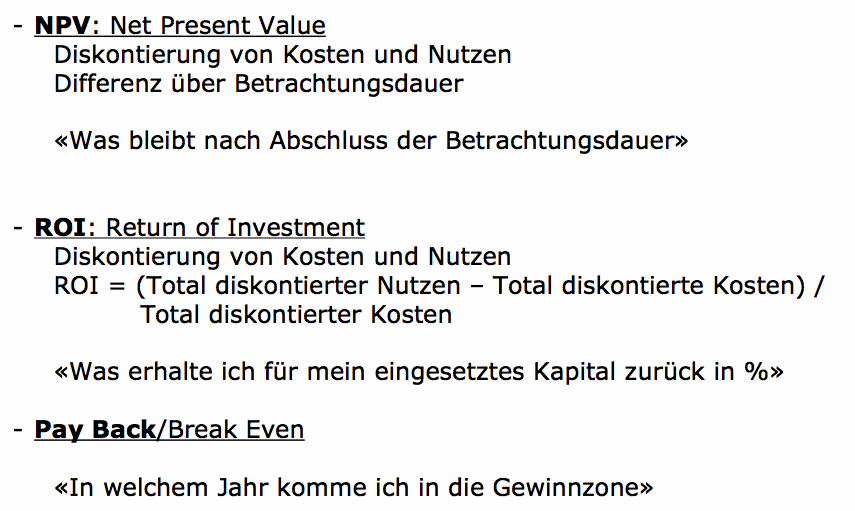
#### Benefits

* Kosteneinsparung: z.B. durch weniger Kundenanfragen über Telefon
  + Community lösen Probleme anderer Kunden
  + Service kann die Erkenntnisse der Community nutzen
* Einnahmesteigerung durch verbesserte Kundenzufriedenheit
* Product Development durch neue Ideen der Community
* Marketing & Sales durch Mund-zu-Mund-Propaganda

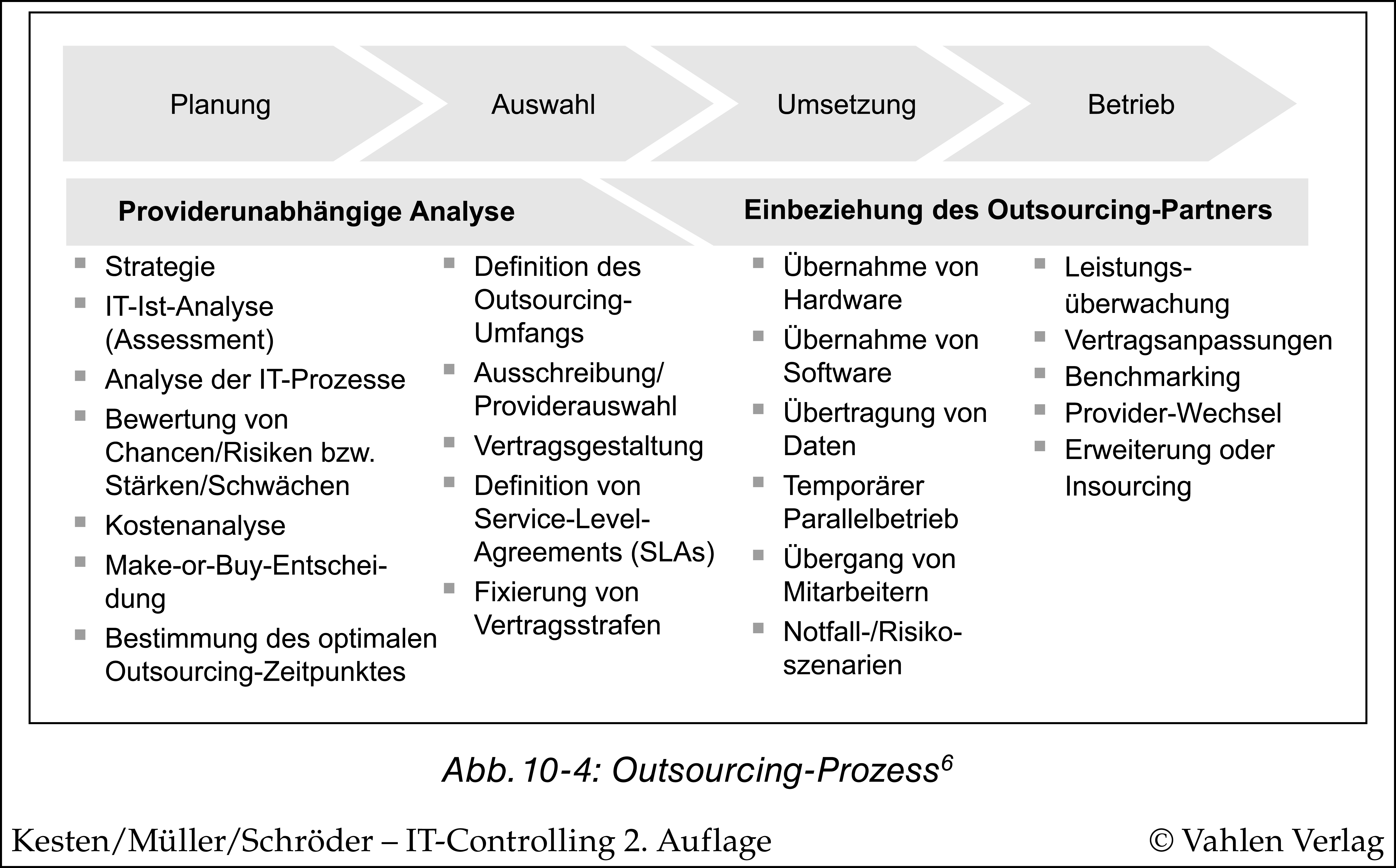
#### Costs

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

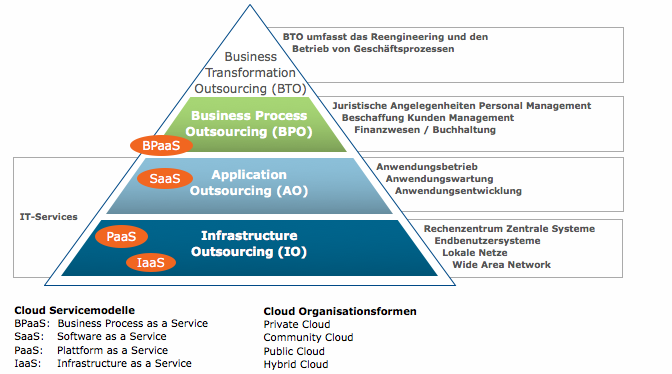
### Finanzielle Kennzahlen



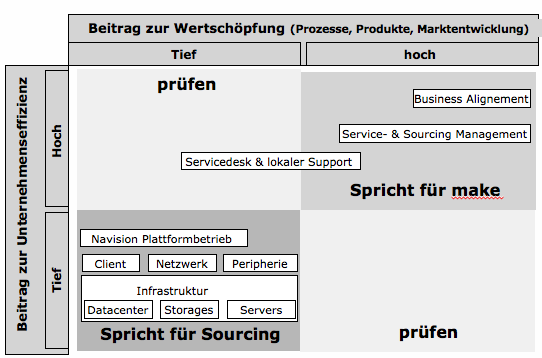
## Outsourcing

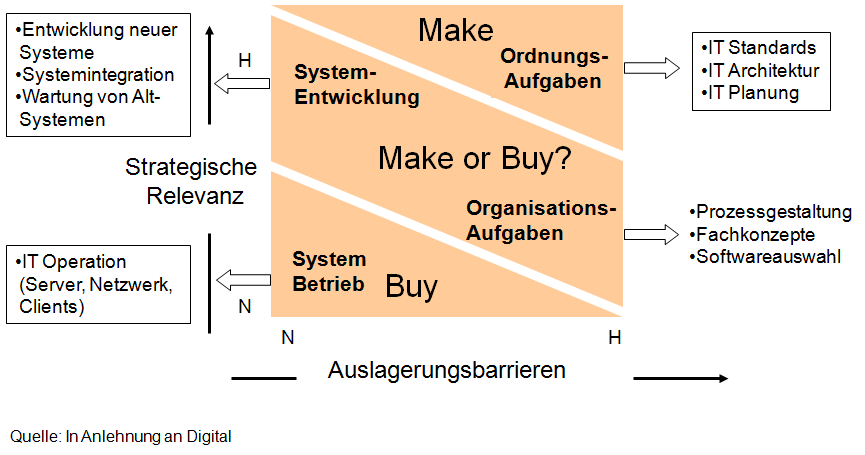


### Formen des Outsourcings

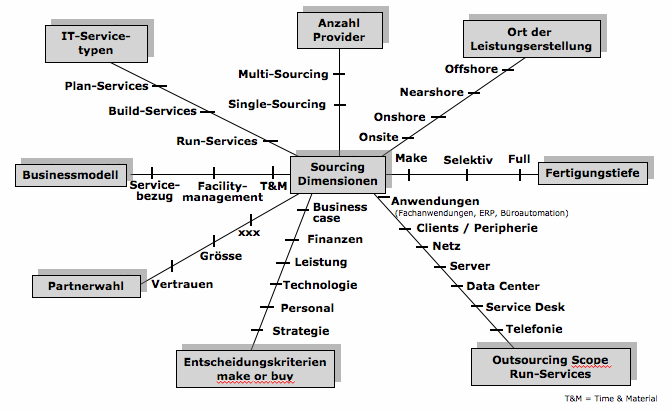


### Bewertung für mögliche Outsourcing-Kandidaten

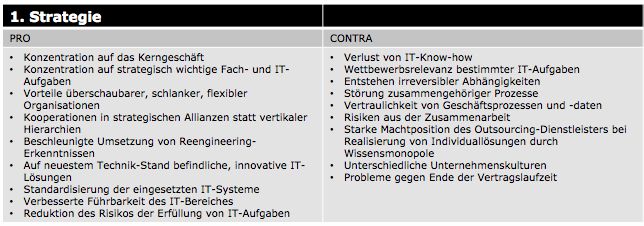


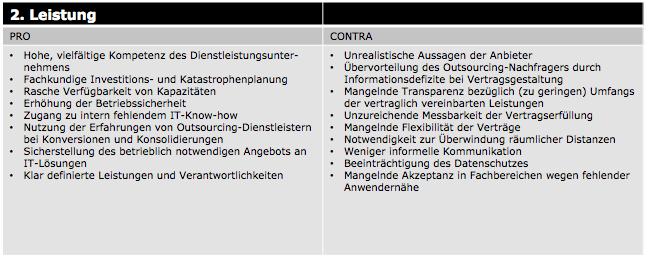


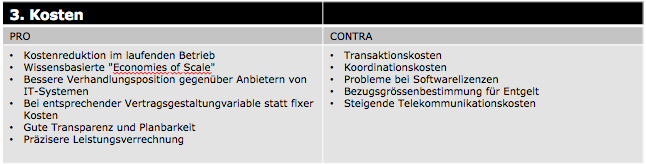
### Prinzipien

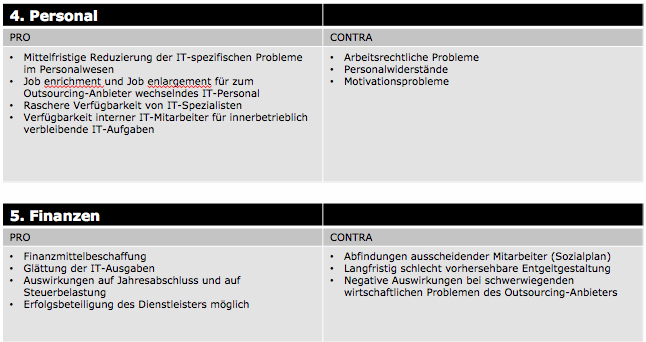


### Argumentenbilanz zum Outsourcing





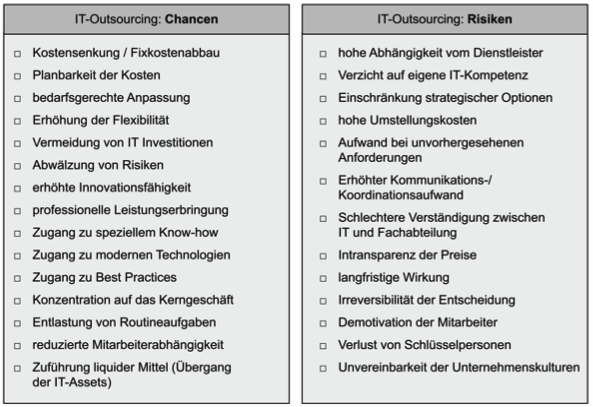




### Erfolgsfaktoren von Sourcing

* Strategie
* Governance
* Ausschreibungsunterlagen
* Vertrag & SLA
* Beziehungsmanagement

### Chancen und Risiken



## Hotelplan

### IT als Business Enabler

3 Trends:

* Entbündelung und Online Zugang
* Polarisierung (Von Normalferien zu vermehrten Billigferien und aussergewöhnlichen Ferien)
* Überkapazitäten (Kapazitäten steigen durch Investitionen 🡪 Kunde am längeren Hebel 🡪 Preisdruck)

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) innert 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)

### Spannungsfeld zwischen Innovation und Kostendruck

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

* Abschreibung
* SW Unterhalt
* Support
* Operations (Data Centers, Infrastruktur, Manpower)

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?)

### 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.

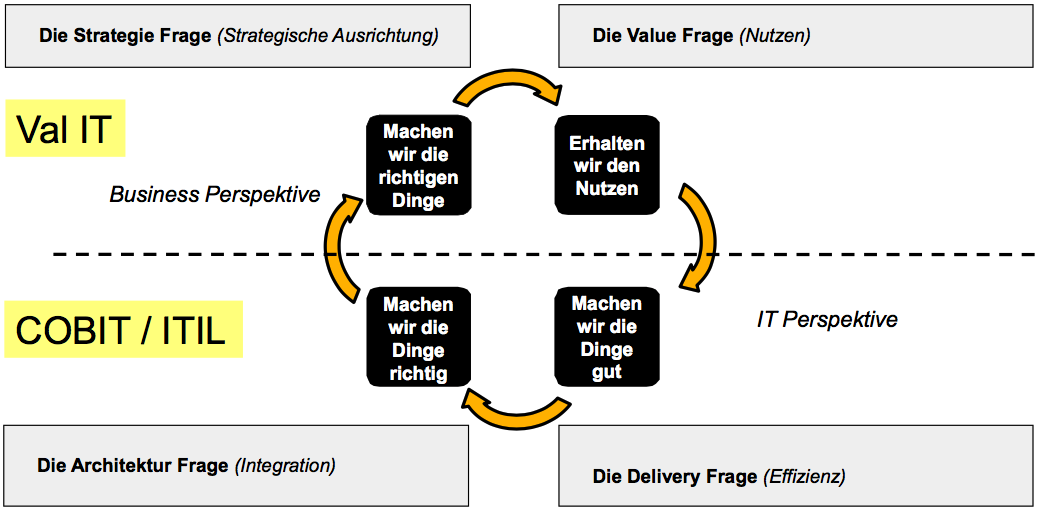
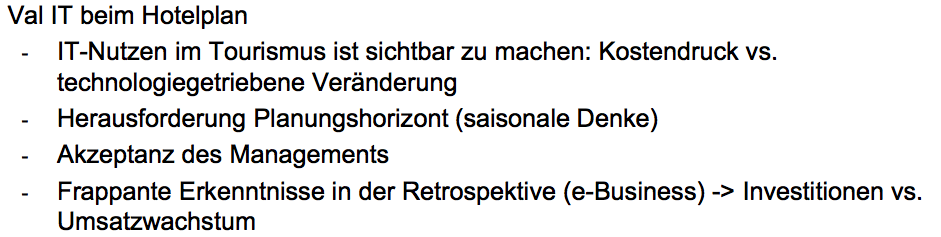


Abbildung Die 4 zentralen Fragen

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

* **Governance Value** (Strategische Dimension): Praktiken zum Nutzenmanagement sind im Unternehmen verankert, um einen optimalen Nutzen über den gesamten Lebenszyklus eines IT-bezogenen Investition zu erzielen.
* **Portfolio Management** (Taktische Dimension): Der Optimale Nutzen soll über das gesamte Unternehmensportfolio an IT-bezogenen Investitionen generiert werden.
* **Investment Management** (Operative Dimension): Die einzelnen IT-bezogenen Investitionen des Unternehmens sollen einen optimalen Nutzen liefern.

Anhand der Hotelplan ICT wurden grob folgende Schritte gemacht:

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

### Zusammenfassung

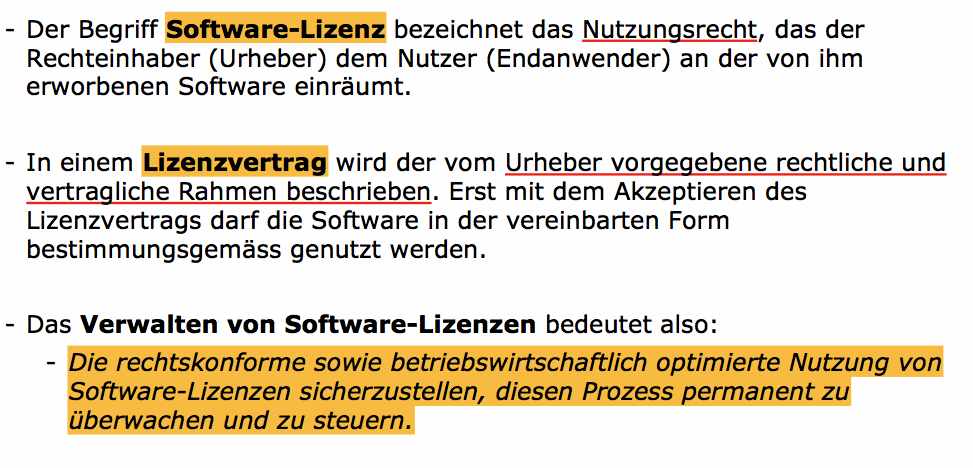
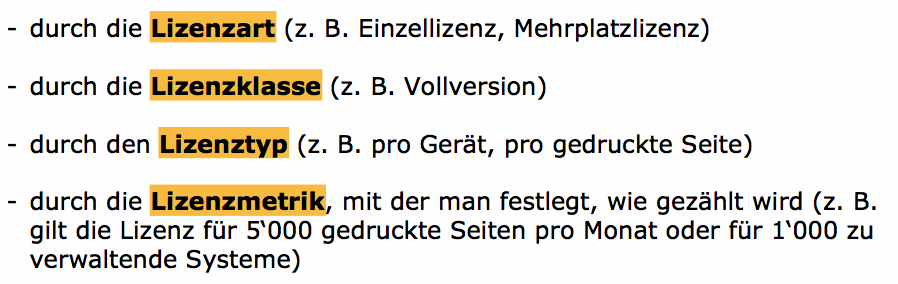
* ICT ist in der Tourismus Industrie mehr als ein Kostenfaktor
* Die Position des Business Enablers (bis hin zum Business Innovator) ist zu erarbeiten
* Nutzen muss ausgewiesen werden
* Val IT ist ein unterstützendes Framework zum strukturierten Umgang mit nutzenorientiertem Investitionsmanagement

## Lizenzmanagement

### Nutzen

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.

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



### Reifegradmodell

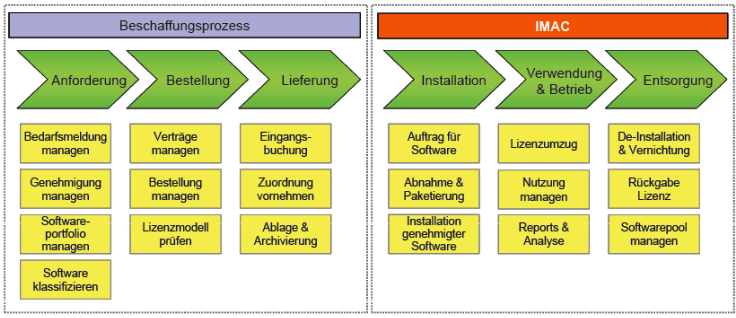
Nach ISO 19970-4 gibt es folgende Stufen zur Einführung:

1. Erzeugung verlässlicher Daten (Compliance Report) 🡪 Exakte Anzahl eingesetzter Software, Anzahl vorhandenen Lizenzen
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 über Lizenzmanagement, dann ist es häufig zu spät.

* Pareto-Prinzip: Mit 20% Aufwand 80% abdecken 🡪 Mit den grossen Softwares anfangen

### Software Life Cycle



### 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

# Max Zeilinger

## Planung

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

### Prüfungsstandard 200

Ziel und allgemeine Grundsätze der Abschlussprüfung

* Überprüfung ob der Abschluss wesentliche Fehlaussagen enthält
* Abschlussprüfung regelt gesetzliche Vorschriften
* Keine systematische Suche nach Gesetzesverstösse
* Es soll mit angemessener Sicherheit festgestellt werden, dass der Abschluss keine wesentlichen Fehler enthält

### Prüfungsstandard 400

Risikobeurteilung und interne Kontrolle. Verständnis für folgendes:

* Des Rechnungswesen Systems
* Der internen Kontrollen
* Des Prüfungsrisikos
  + Inhärentes Risiko: Risiko, dass eine bestimmte Abschlussposition wesentliche Fehlaussagen enthält
  + Kontrollrisiko: Risiko, dass inhärentes Risiko durch RW-System und internen Kontrollen nicht verhindert
  + Aufdeckungsrisiko: Risiko, dass die Prüfungshandlung eine Fehlaussage nicht aufdecken kann

Planung der Prüfungshandlung damit das Prüfungsrisiko auf ein akzeptables Niveau verringert wird.

### Prüfungsstandard 401 (Umfeld der IT)

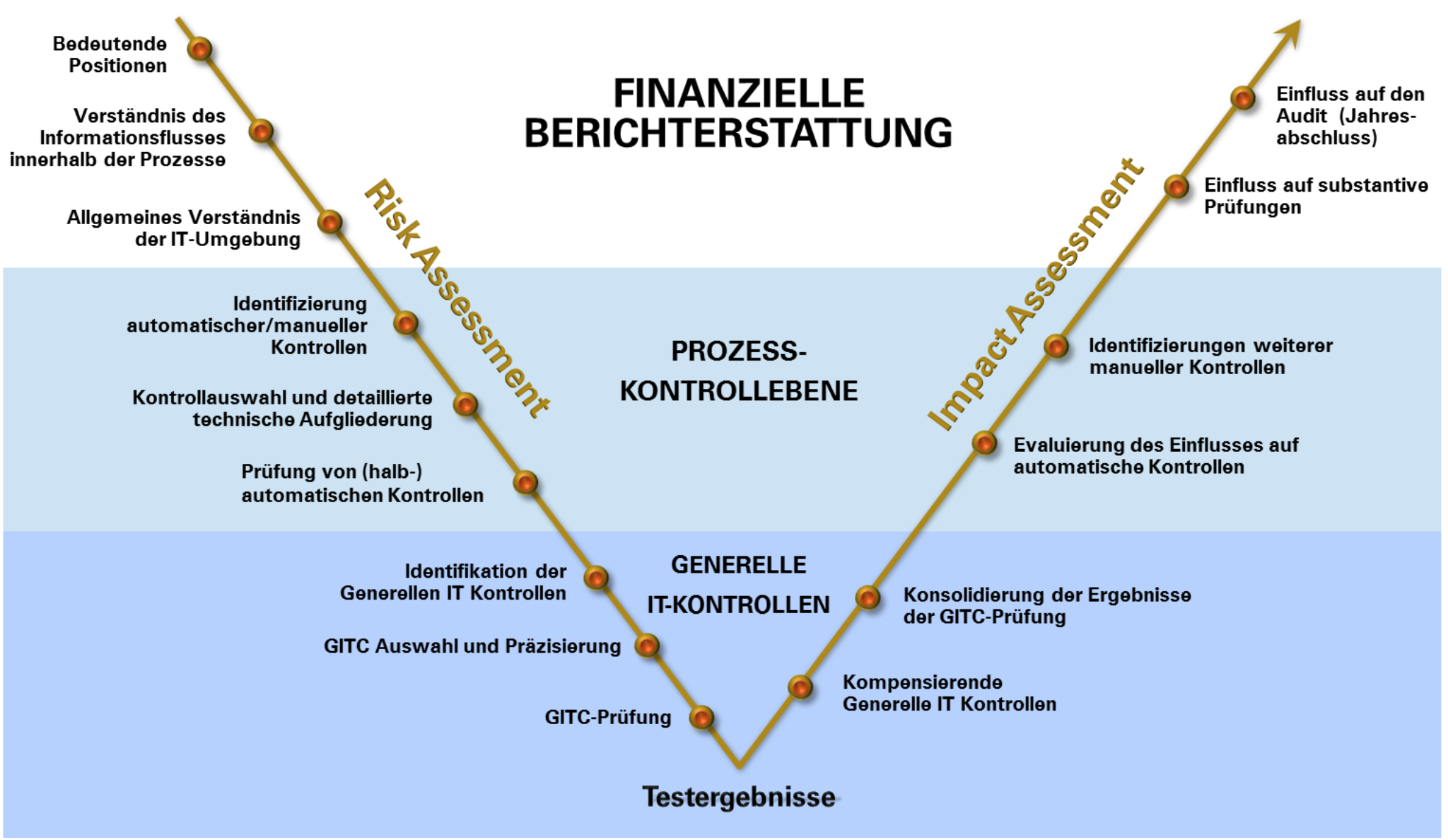
Es sind IT Kenntnisse erforderlich, ggf. müssen Experten zugezogen werden.

### Revisionsstrategie

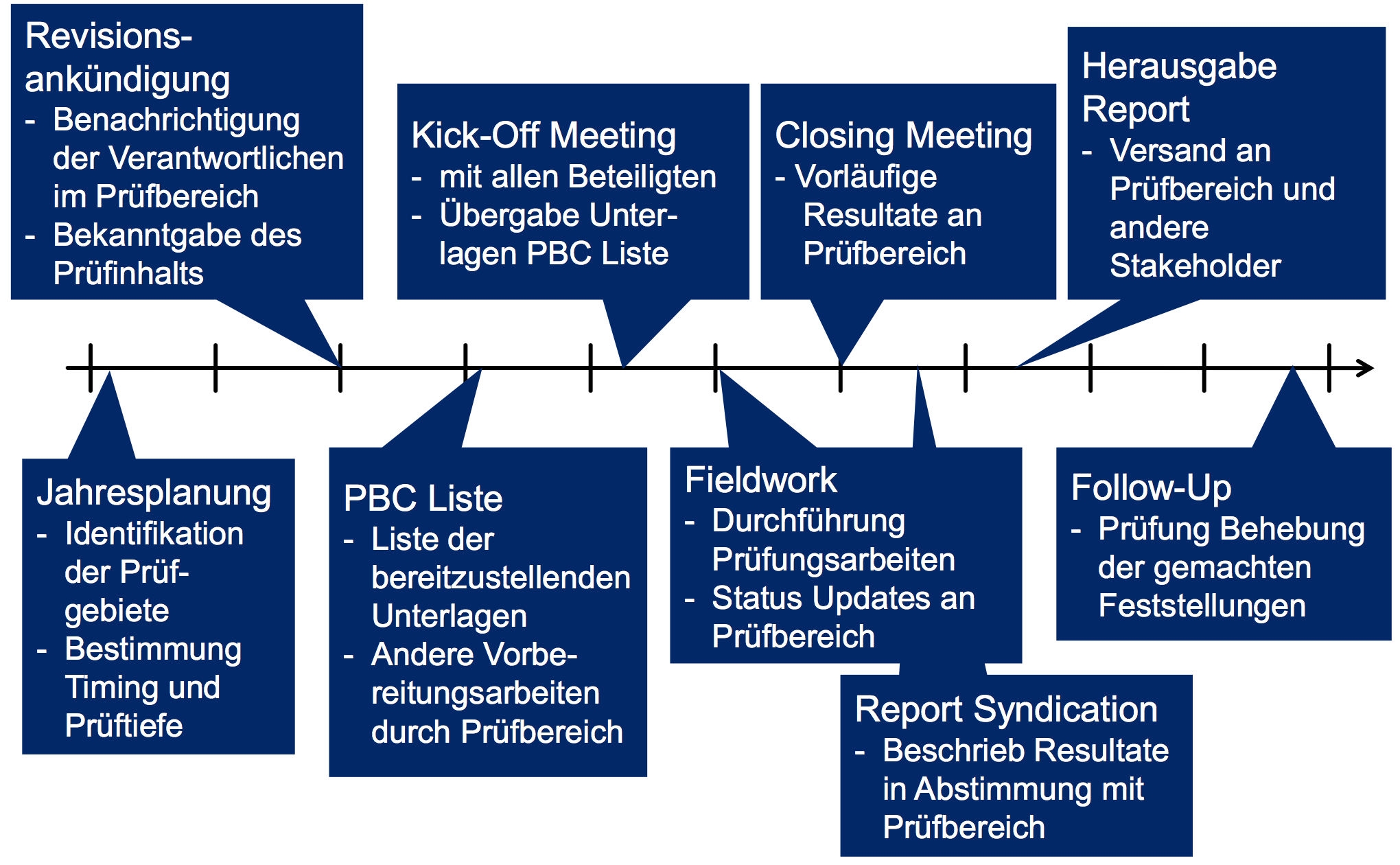
* Bestätigung der Jahresrechnung (Financial Statement Audit)
* Prüfung ob eine Systemmigration erfolgreich durchgeführt wurde und alle Daten vollständig und korrekt übertragen wurden (Migrationsprüfung)
* Bestätigung das bei einem Dienstleistungserbringer angemessene Kontrollen existieren (Service Provider 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** |
| **1** | Effektivität | Effektivität und Effizienz |
| **Prüeftiefe** | Prüfung der wesentlichsten Punkte | Oftmals Deep Dive in ein spezielles Thema |
| **Scope** | Materiell für Finanzberichterstattung | Alle Unternehmensbereiche |



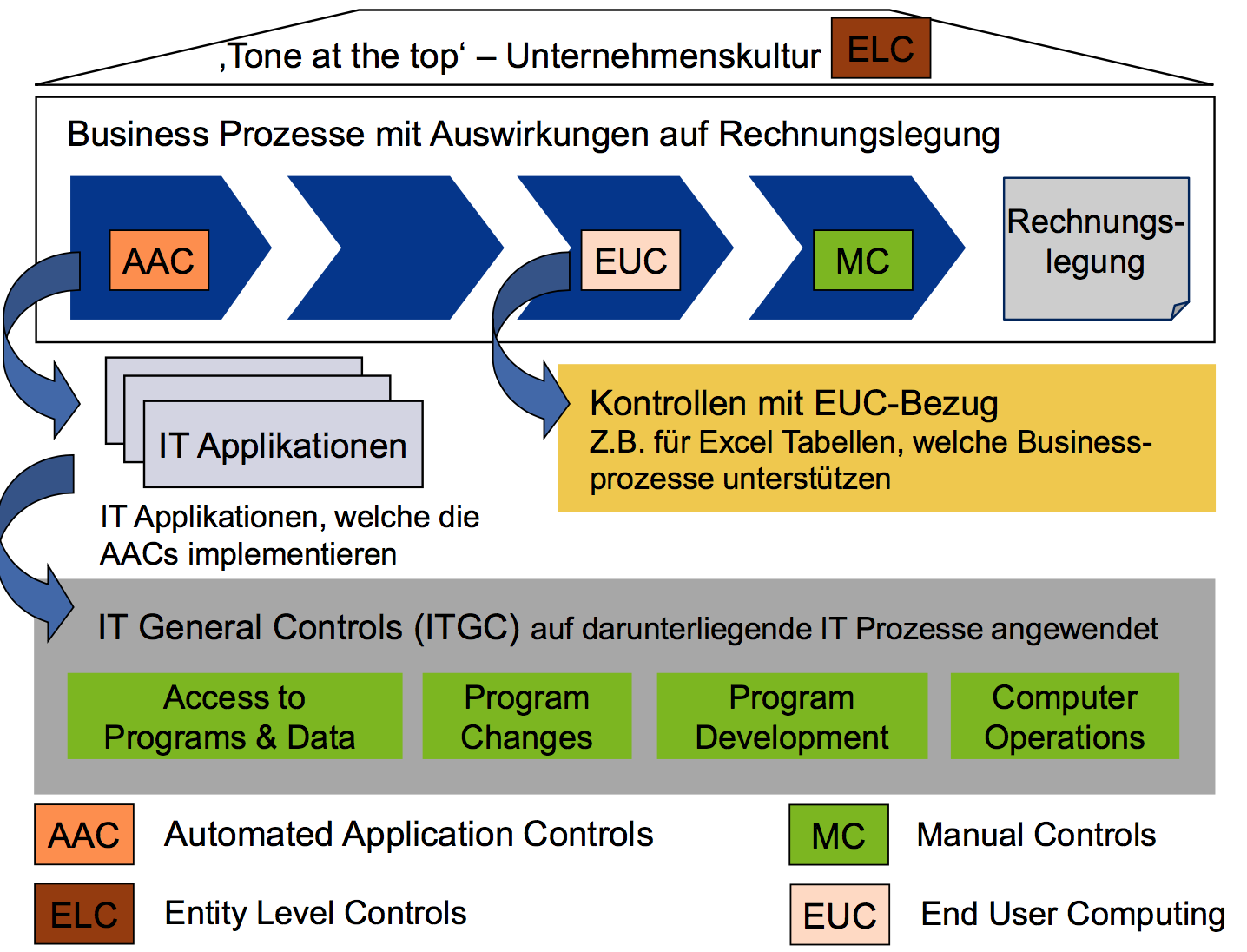
### Prüfungsorganisation



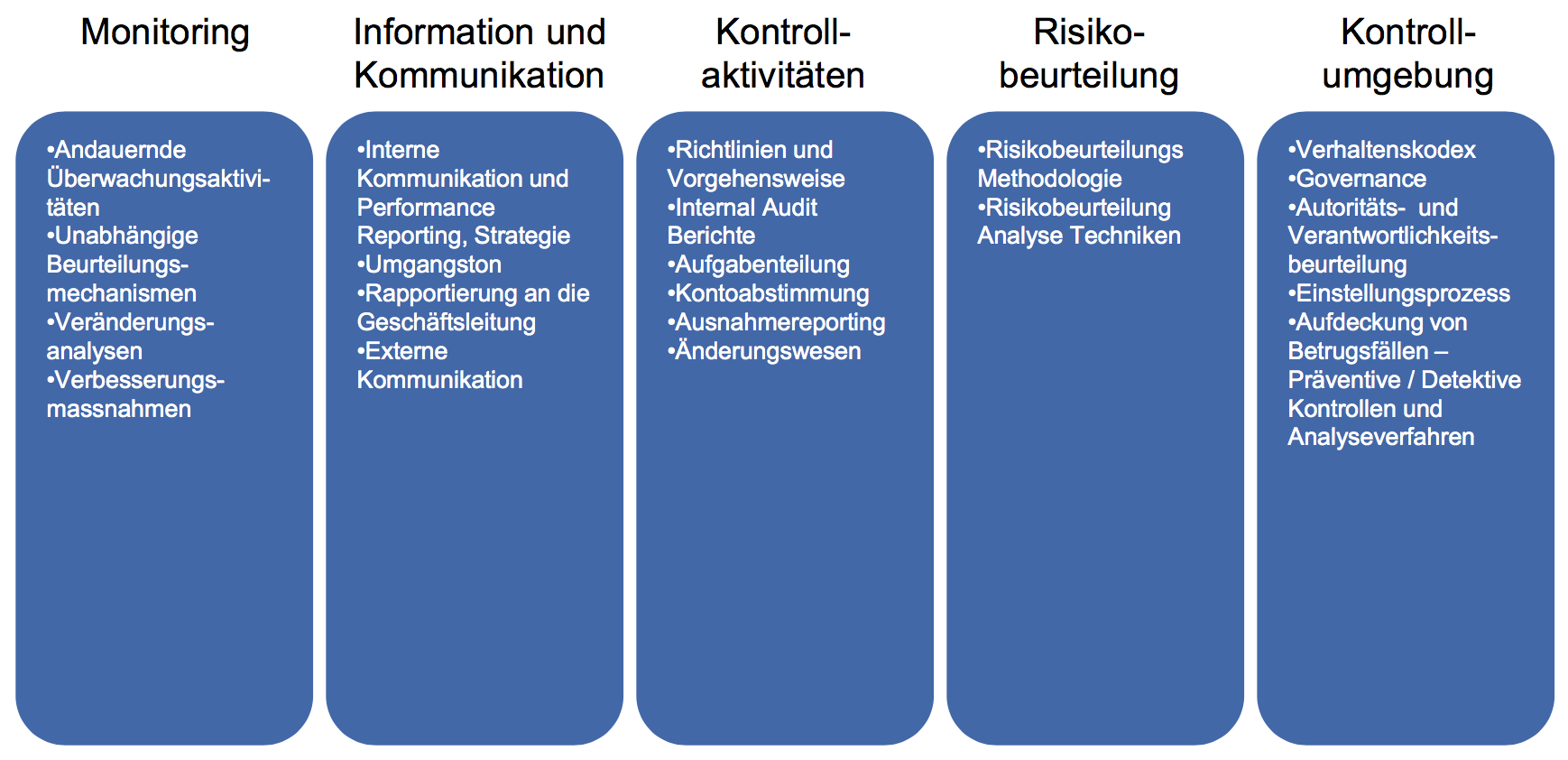
Vorgehen bei der Erstellung von Audit Report:

* Audit Reports können direkte Auswirkungen auf den Bereich/Person haben
* Der Inhalt des Berichts muss akzeptiert werden
  + Inhaltliche Korrektheit
  + Wording akzeptabel
  + Fristen für Behebung machbar
  + Zuordnung Verantwortlichkeiten für Feststellung und Behebung korrekt

## Prüfungsdurchführung



### 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. Es geht darum zu prüfen ob ausreichende Kontrollen über die Unternehmenskultur und Leistungserbringung bestehen. Es ist ein Top-Down-Approach bei den Richtlinien und deren Umsetzung überprüft werden.

### Process Level Controls

Können automatisiert oder manuell durchgeführt werden. Es gibt 3 Typen:

* Eingabekontrollen (Input Autorisierung, Batch Kontrollen, Exception Reporting)
* Verarbeitungskontrollen (Datenvalidierung, Programmprüfungen, Abstimmungen, Exception Reporting)
* Ausgabekontrollen (Logging und Archivierung, Reportverteilung)

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

* Vollständigkeit (Completeness)
* Genauigkeit (Accuracy)
* Existenz (Existency)
* Valuation (Bewertung, Wertung) 🡪 Wirtschaftsprüfung
* Obligations and rights (Verpflichtung und Rechte) 🡪 Wirtschaftsprüfung
* Presentation and disclosure (Einordnung und Ausweis) 🡪 Wirtschaftsprüfung

### Generelle IT Kontrollen

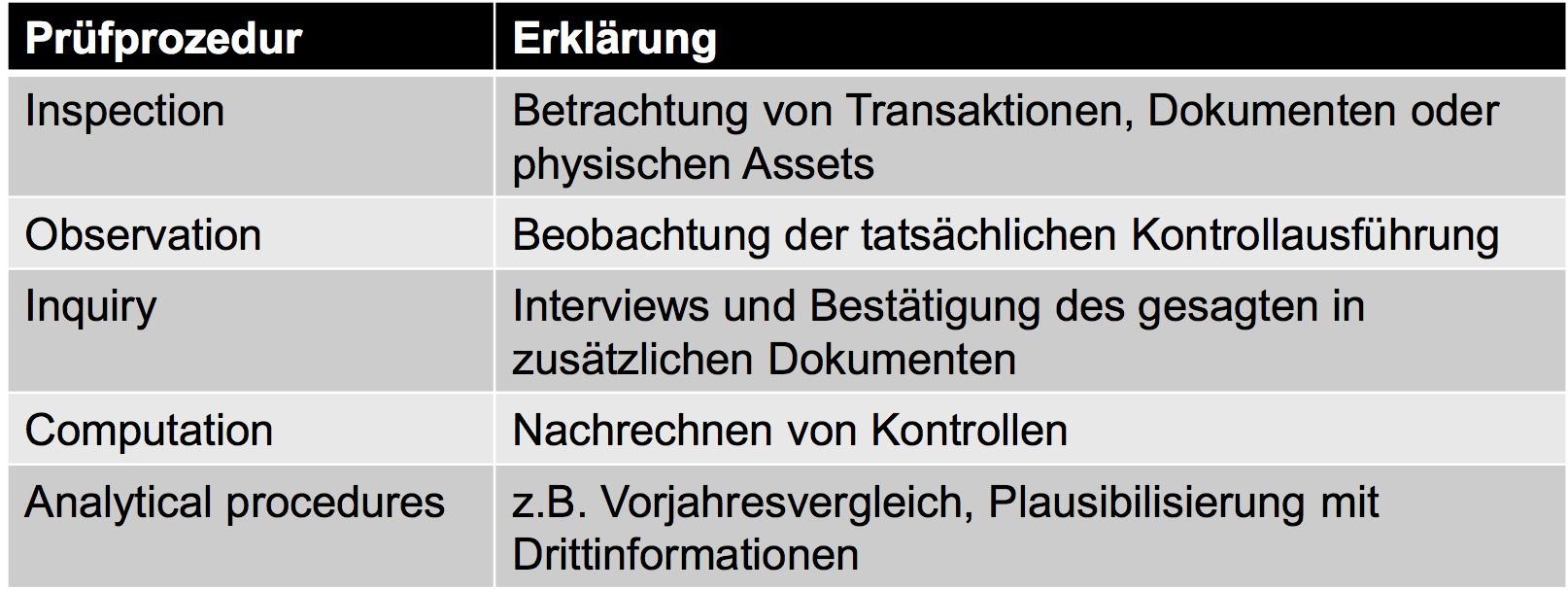
Sind für alle Prozesse und Bereiche relevant. Unterstützten das Funktionieren von PLC über die ganze Prüfperiode, stellen Grundsicherheit für die zu prüfende IT, Tiefe hängt von den PLC ab.

Prüfbereiche sind:

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

### Prüfprozeduren

Folgende Prüfprozeduren können ausgeführt werden, um die Assertions abzudecken.



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

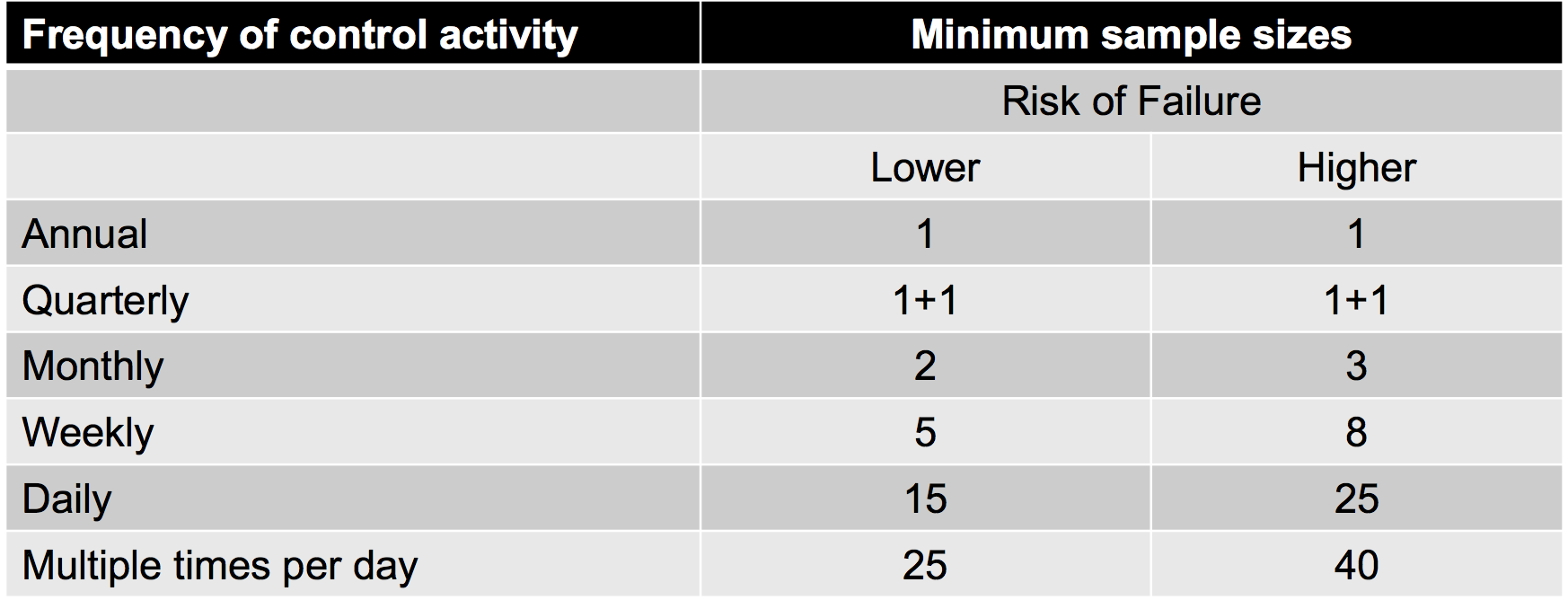
### Manuelle Kontrollen

* Menschliche Komponente –> schwieriger einzuschätzendes Kontrollrisiko, abhängig von:
  + Kompetenz
  + Objektivität des Kontrolldurchführenden
* Qualitätsschwankungen bei verschiedene Kontrolldurchführende
* Operationelle Effektivität durch Stichprobenprüfung
* Meist aufwändiger als Automatische

Zum Beispiel Reviews von Berechtigungen oder Bewilligungen durch Vorgesetzte

#### Stichprobenprüfung

* Statistical Samping
  + Attribute Sampling (Vorkommen eines bestimmten Werts
  + Variable Sampling (Wertbasiert z.B. Schätzung des Werts)
* Non-statistical Sampling (Basierend auf Erfahrung des Auditors)
* Stratified Sampling (Mischform)



### 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

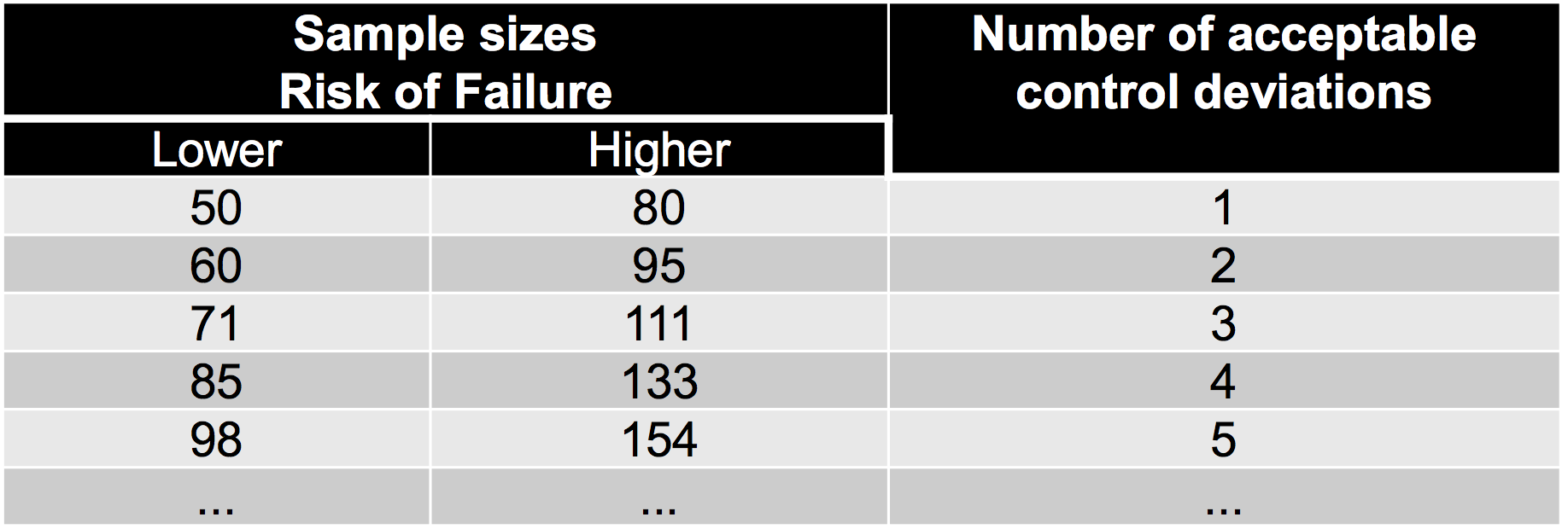
#### Test of One

* 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.

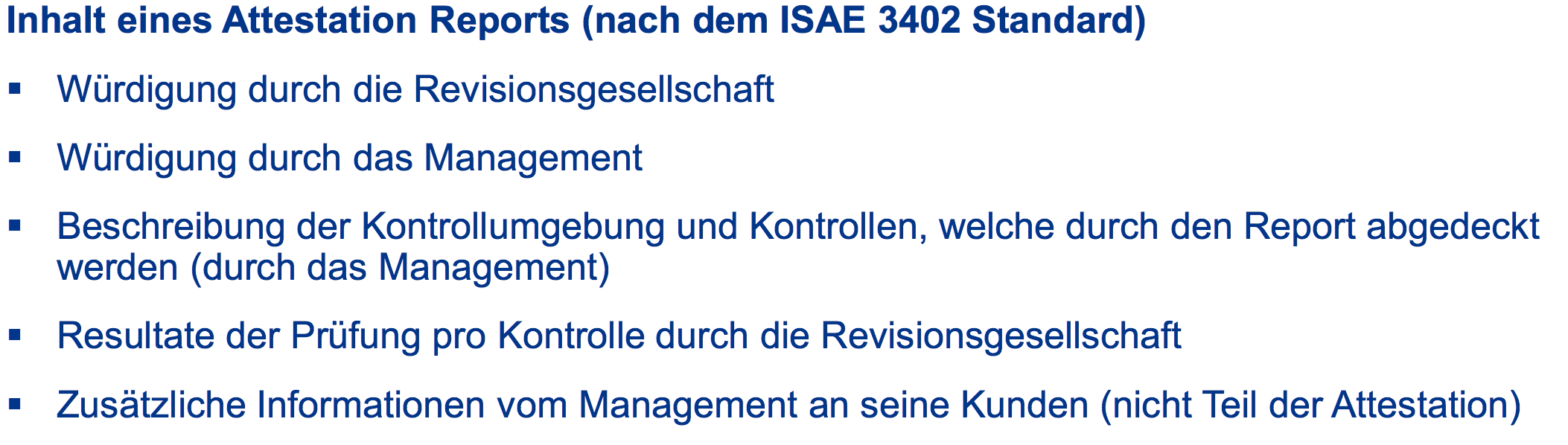
### Verhalten bei Exceptions

* Bei Automatischen Kontrollen muss der Test als nicht effektiv beurteilt werden.
* Bei Manuellen Methoden 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.



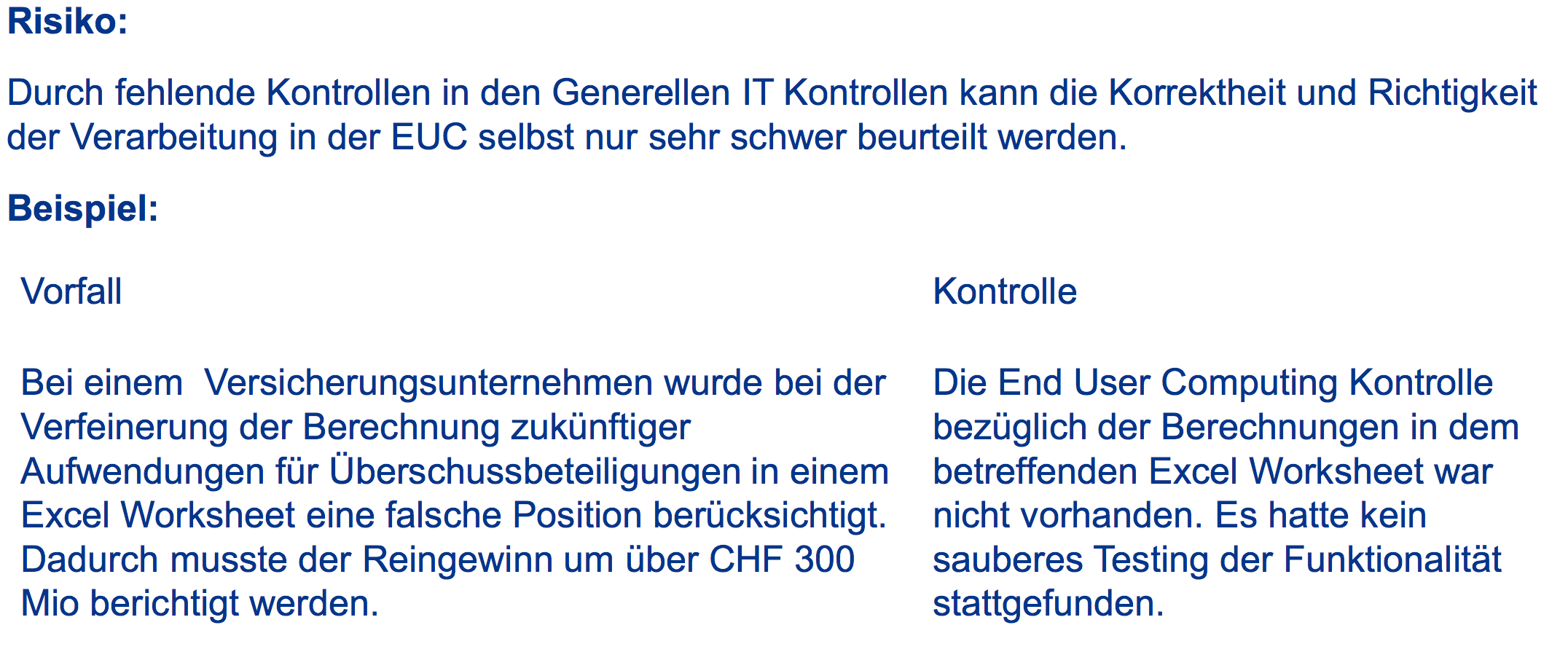
### Attestation Reports

Überprüfung der Kontrolle durch einen externen Dienstleister. Ein Attestation Report macht entweder nur eine Aussage zum Design der Kontrollen oder auch zu ihrer Operativen Effektivität.



### 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. Applikationsfunktionalitäten in Excel oder Access.



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 eienr 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

#### Individuelles Testen

* Zugriff auf EUC Applikation
  + Schutz des Ordners, wo die Applikation abgelegt ist
  + Zugriffschutz 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

## Frameworks

### ISACA

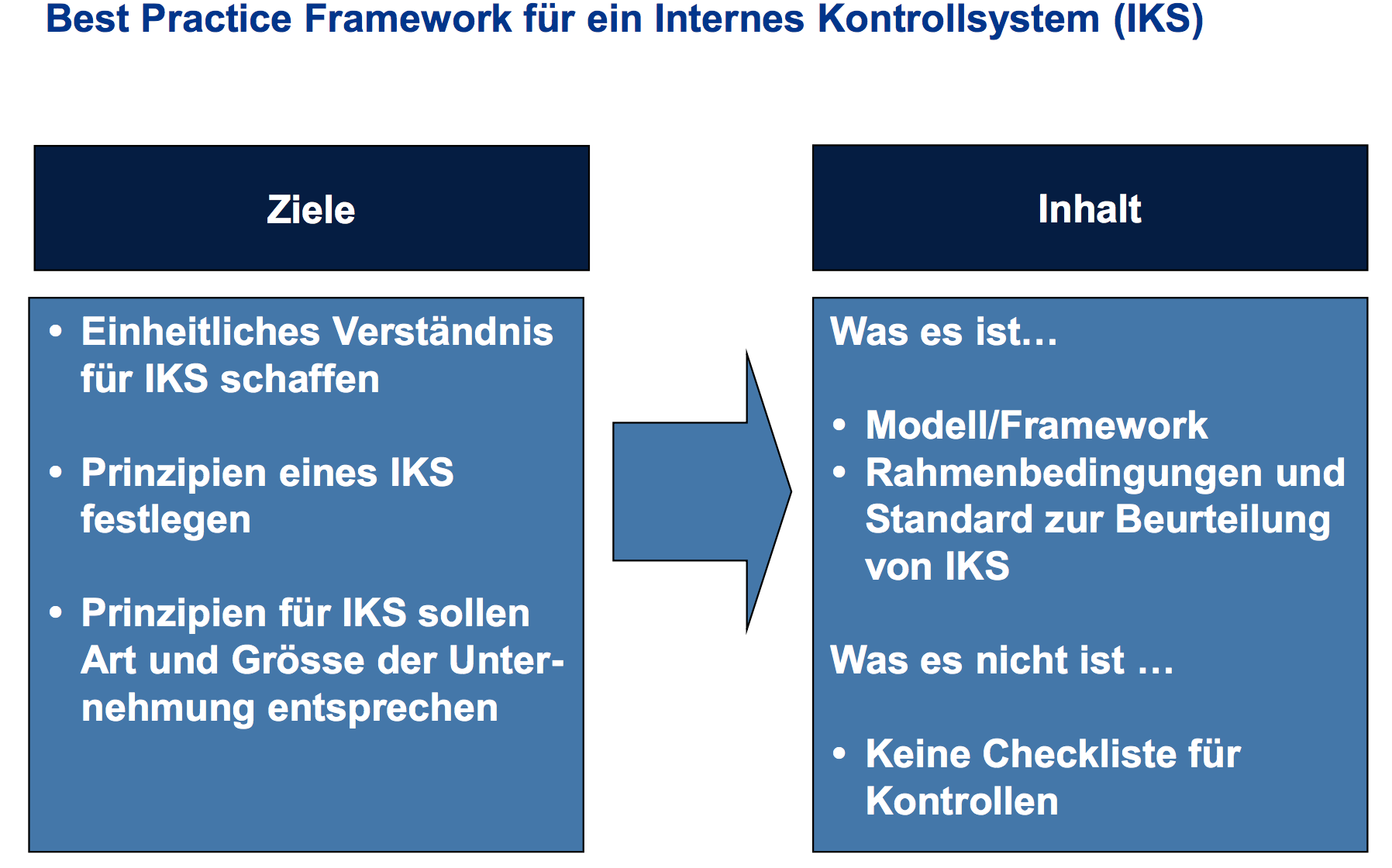
Information Systems Audit and Control Association

* 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

### 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



## Dokumentation

* Dokumentation muss einen fachkundigen Dritten erlaube, 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
  + Erzwingung der 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

## Bewertung Ergebnisse

* Kontrolle ist in ihrem Design nicht geeignet, die Kontrollzielen abdzudecken 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

### Einzelne ineffektive 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

Bei vollautomatischen Kontrollen liegen Design und operative Effektivität sehr nahe beieinander. Wenn 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?
* 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)

Mit Computer Assisted Audit Techniques (CAATs) können nicht nur vollständig ergebnisorientierte Prüfungen durchgeführt werden, sondern auch die Einhaltung von Kontrollzielen überprüft werden. Bsp. Gewaltentrennung für sämtliche vergebenen Benutzerrechte

### Inneffektive 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, 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.

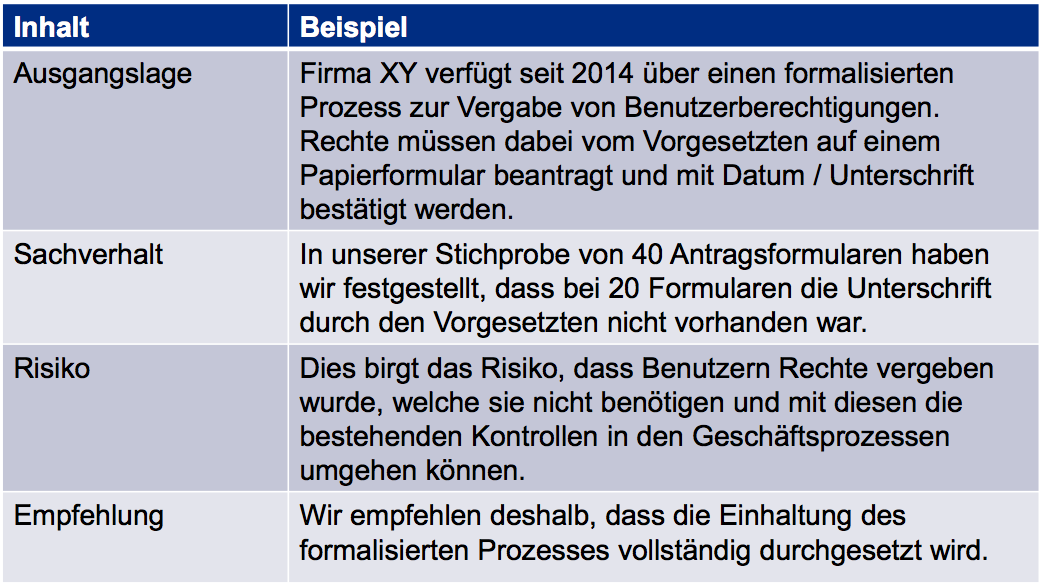
### Ineffektive Generelle IT Kontrolle (Einzel)

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.

## Herleitung Massnahmen



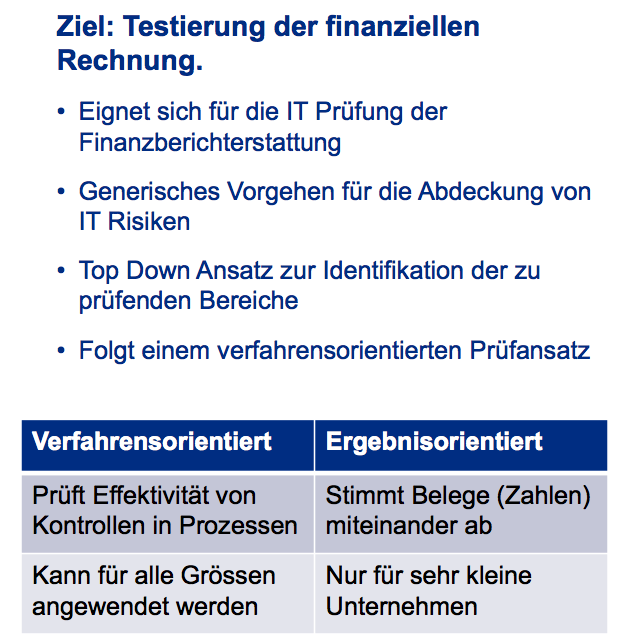
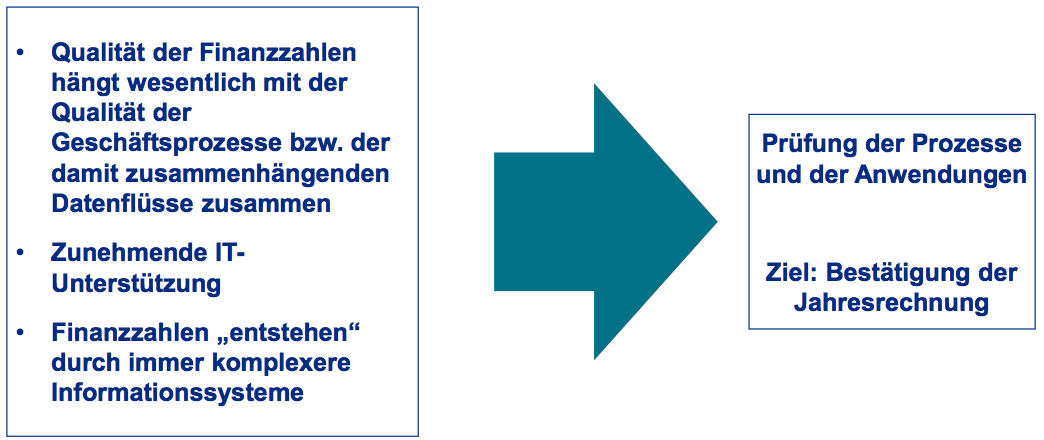
Der Weg von einer festgestellten Ausnahme bis zur akzeptierten Feststellung im Bericht kann sehr lang sein

* 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
  + Kurzbeschreib 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
* Nicheinhaltung der Umsetzung / Termine wird von vielen Unternehmen intern massiv bestraft
* Unterscheidung mit Repeat Issues, welche noch nicht behoben werden mussten

## Vorgehensmodell der Schweizer Treuhand-Kammer



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-Trough
6. Beurteilung des Kontroll-Designs
7. Beurteilung der Umsetzung der Kontrollen
8. Gesamtbeachtung und Ergebnisfindung

