HOCHSCHULE HEILBRONN

› GRUNDLEGENDE ASPEKTE DES IT-MANAGEMENTS

Einführung IT-Management | Philipp Küller, Wirtschaftsinformatik | Sommersemester 2024

AGENDA

I. Grundbegriffe in Bezug auf das IT-Management

II. IT-Organisation

III. Sourcing Modelle

IV. Personal und Leadership

V. Compliance, Rechtsfragen & Normung

VI. Sicherheit und Datenschutz

WAS SOLL IN DIESEM KAPITEL VERMITTELT WERDEN

Was versteht man unter den Grundbegriffen des IT-Managements und wie sind diese definiert?

Welche grundlegenden Organisationskonzepte für den IT-Bereich gibt es (organisatorische Ausrichtung als Cost-, Service- oder Profitcenter, zentrale versus dezentrale Standorte)?

Welcher Umfang an IT-Leistungen sollte durch das Unternehmen selbst erbracht werden, welche sollten aus wirtschaftlichen oder anderen Gründen zugekauft werde?

Wie können Entscheidungen für ein Outsourcing von IT-Aufgaben, IT-Services und IT-Prozessen zweckmäßigerweise erfolgen und erfolgreich umgesetzt werden?

Welche rechtlichen Anforderungen bestehen? Und warum steht ein IT-Leiter immer mit einem Bein im Gefängnis?

› GRUNDBEGRIFFE IN BEZUG AUF DAS IT-MANAGEMENT

GRUNDBEGRIFFE

Folgende übergreifenden Grundbegriffe vorab bzw. als Wiederholung als Basis für die kommenden Lerneinheiten

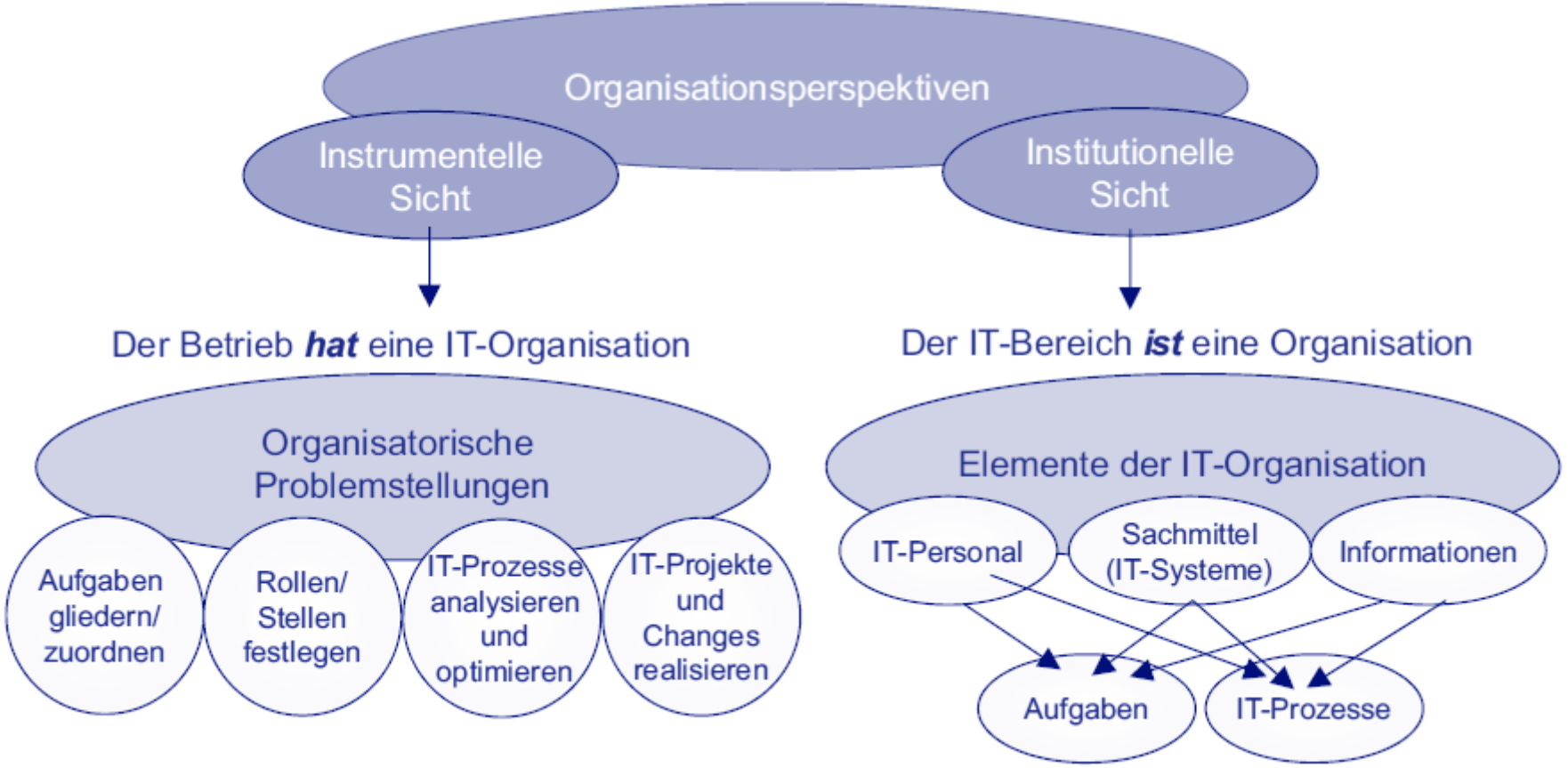
a. Informationssystem
b. Unternehmensarchitektur
c. Prozess (Geschäftsprozess & IT-Prozess
d. IT-Service
e. IT-Asset
f. Service Level Agreement (SLA)
g. Compliance
h. Governance
i. Key Performance Indicator (KPI)
j. RACI-Matrix / RASCI-Matrix

Inhalt erarbeitet als Übung im Rahmen der Veranstaltung!

HOCHSCHULE HEILBRONN

› IT-ORGANISATION

EINORDNUNG DES BEGRIFFS „IT-ORGANISATION“



IT-ORGANISATION

Für kurze Entscheidungswege sowie eine schnelle und fundierte Informationsbeschaffung ist eine adäquate IT-Organisationsform mit klar definierten Rollen und Verantwortlichkeiten entscheidend

Für die Gestaltung einer IT-Organisation betrachten wir aus institutioneller Sicht diese grundlegenden Ordnungselemente:

- Menschen
- Organisationsformen
- Rollen und Verantwortlichkeiten und Skills
- Entscheidungsfelder und Gremien
- Architekturen und Sachmittel
- Informationen

STUFEN DER GESTALTUNG FÜR EINE OPTIMIERUNG DER IT-ORGANISATION

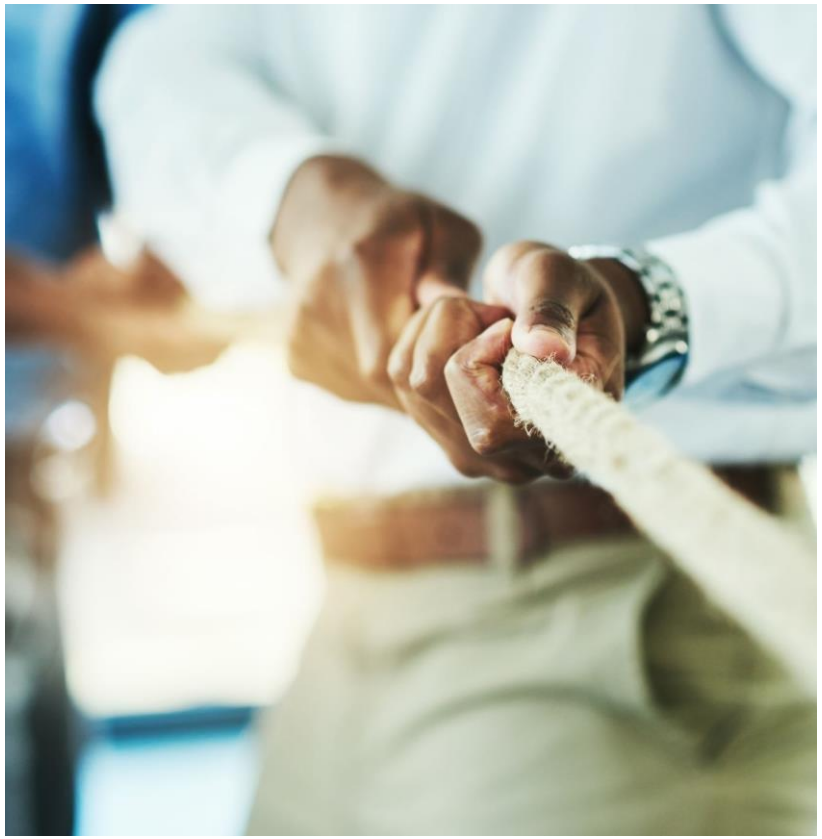
Stufe 1: **Grundsatzentscheidungen** zur Einordnung des IT-Bereichs für ein Unternehmen treffen (etwa hinsichtlich der Kunden und des Leistungsportfolios der IT-Organisation)

Stufe 2: **Aufgaben analysieren** und systematisieren, die in der IT-Organisation anfallen

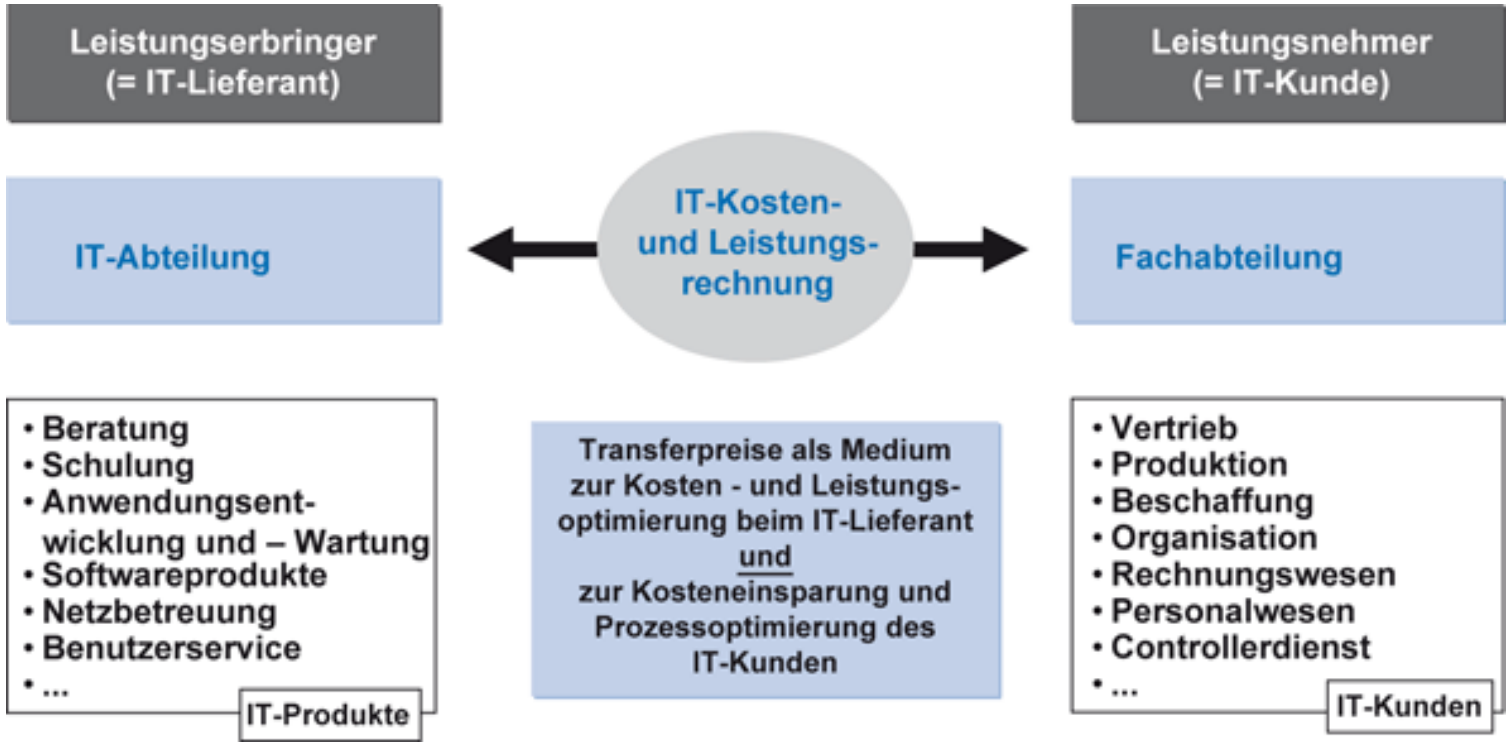
Stufe 3: **Prozesse** der Unternehmens-IT identifizieren, dokumentieren und optimiert gestalten (Management und Governance-Prozesse & IT-Entwicklungs- und Serviceprozesse)

Stufe 4: **Rollen** für die IT-Organisation vereinbaren, definieren und in Prozessen sowie den Stellen zuordnen

Stufe 5: **Konsequenzen** für die Stellen- und Leitungsorganisation ableiten sowie Fragen der **Team- und Gremienorganisation** regeln



EXKURS: LEISTUNGSVERRECHNUNG



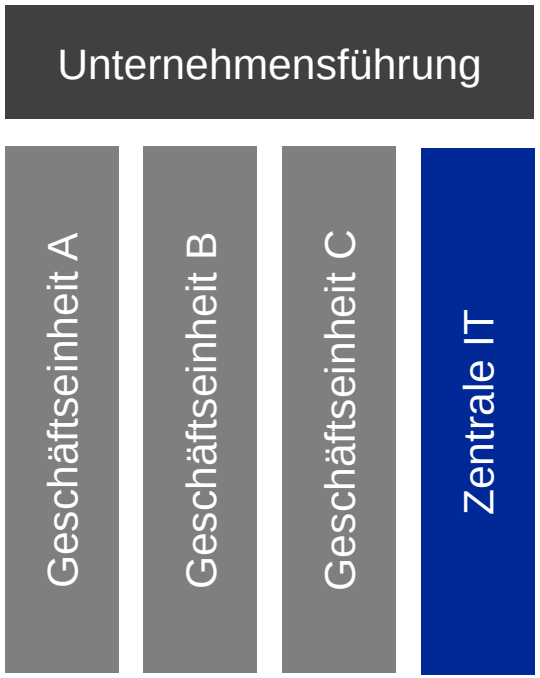
HOCHSCHULE HEILBRONN

ENTSCHEIDUNGSAUTONOMIE IN DER IT-ORGANISATION

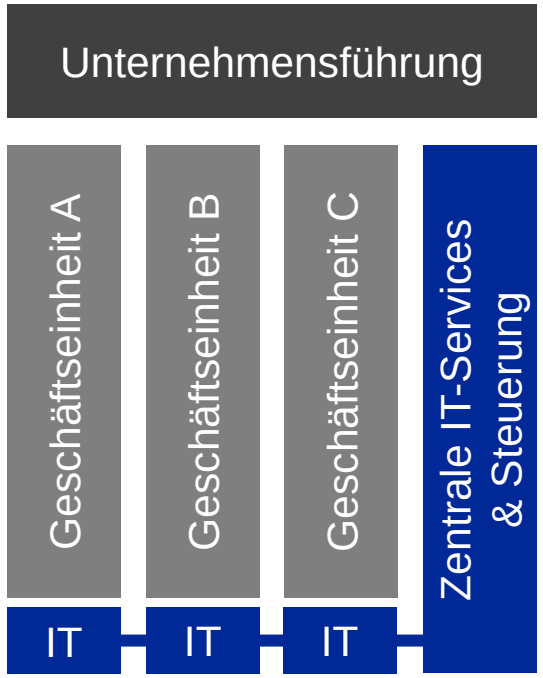
Cost Center	Profit Center	Investment Center	Shared Service Center
Gemessen an der Einhaltung des IT-Budgets	Gemessen am Gewinn / Deckungsbeitrag	Gemessen an der Rendite / dem Wertbeitrag	Gemessen an der Rendite / dem Wertbeitrag oder am Gewinn / Deckungsbeitrag
Entscheidung über Ressourcenverbrauch	Entscheidung über Ressourcenverbrauch und Erlöse	Entscheidung über Ressourcenverbrauch, Kapazitäten, Investments und Erlöse	Entscheidung über Ressourcen-verbrauch, Kapazitäten, Investments und Erlöse / Entscheidung über Ressourcen-verbrauch und Erlöse
Keine Entscheidung über Erlöse und Vorgaben zu Kapazität und Budget	Vorgaben zu Kapazitäten		Vorgaben zu Kapazitäten
Ziel: Einhaltung von Plankosten bzw. eine Kostenminimierung bei einem bestimmten Leistungsumfang	Ziel: Ermittlung des der IT-zurechenbare wirtschaft-lichen Ergebniss (d.h. Gewinn & Rentabilität der IT)	Ziel: „Unternehmen im Unternehmen“ – Ausprägung der Eigensteuerung und Verantwortung der IT	Ziel: Dienstleister für mehrere Unternehmensteile unter Ausnutzung von Ressourcen- & Standardisierungsvorteilen

ORGANISATIONSFORMEN

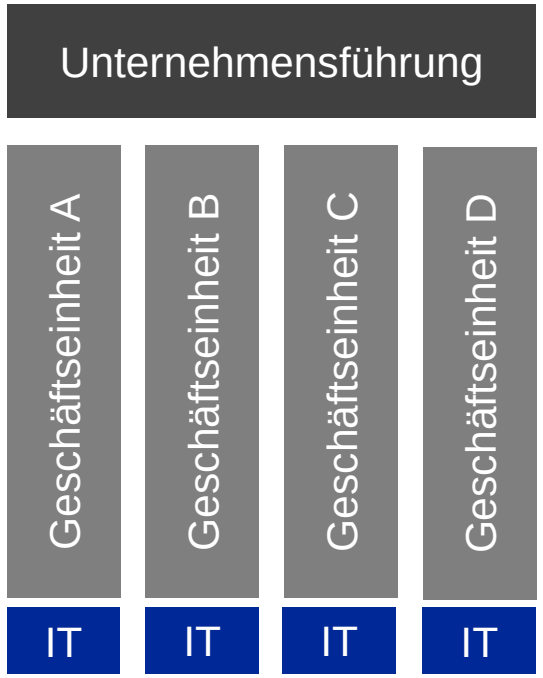
Zentralisierte Aufstellung einer IT-Funktion



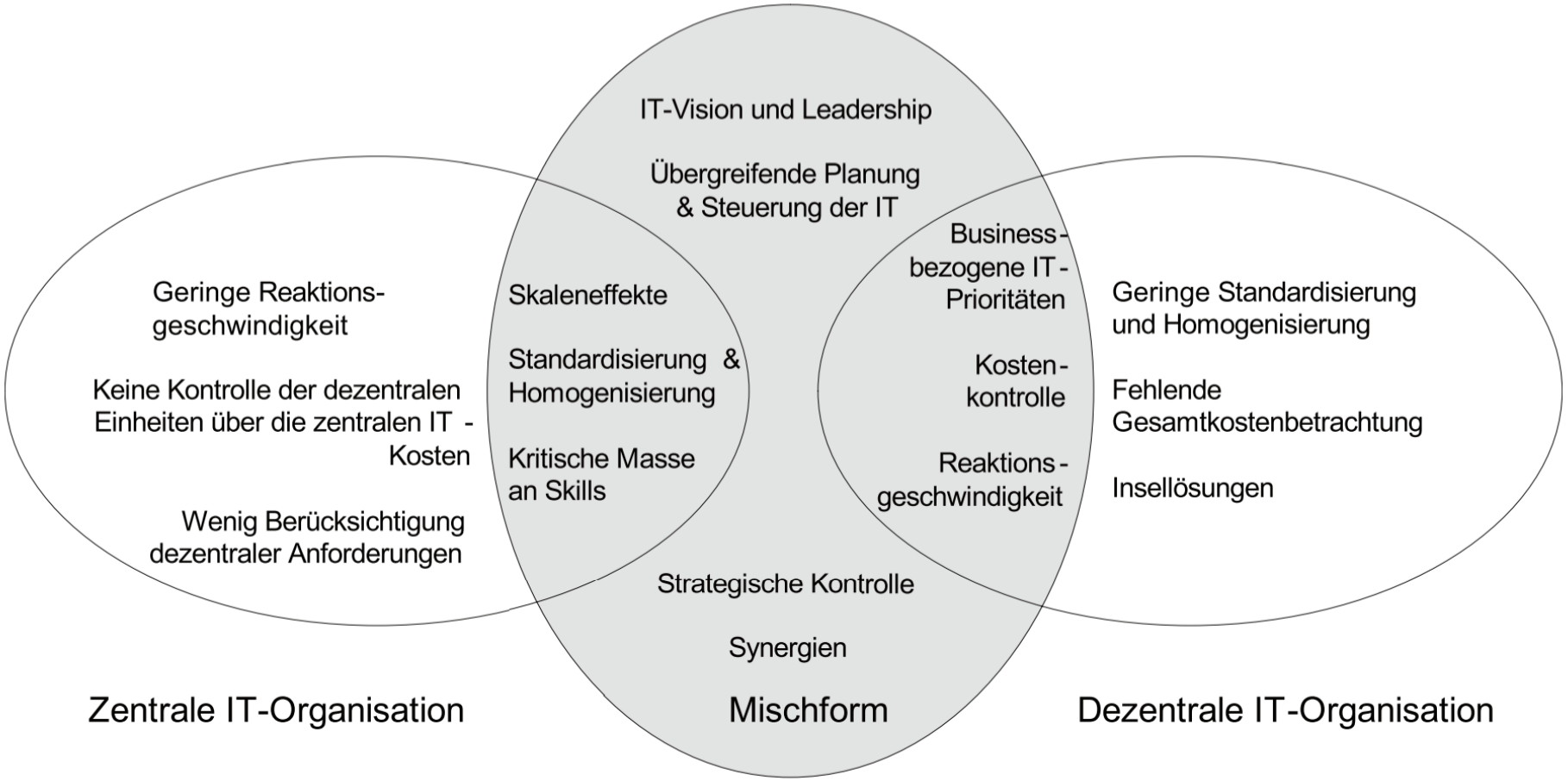
Hybride Aufstellung der IT-Funktionen (Mischform)



Dezentrale Lokalisierung aller IT-Funktionen



ORGANISATORISCHE ASPEKTE
ZENTRAL VS. DEZENTRAL VS. MISCHFORM

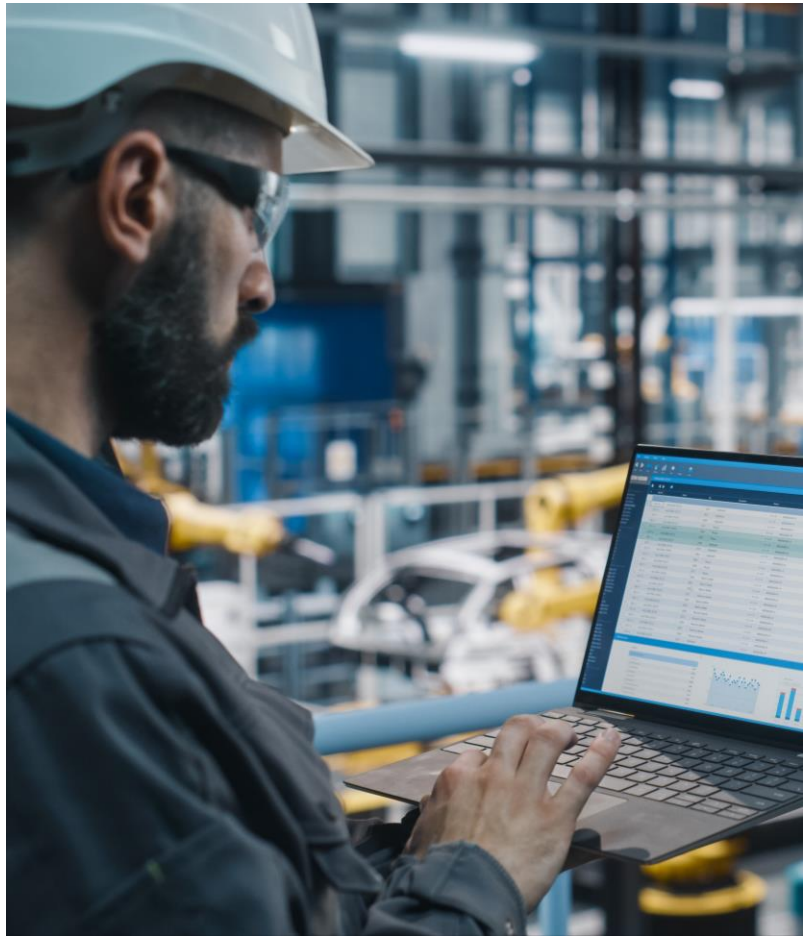


ÜBUNGSAUFGABE 7-MINUTEN
ZWEIERTEAMS

Scenario „Maschinenbauer“

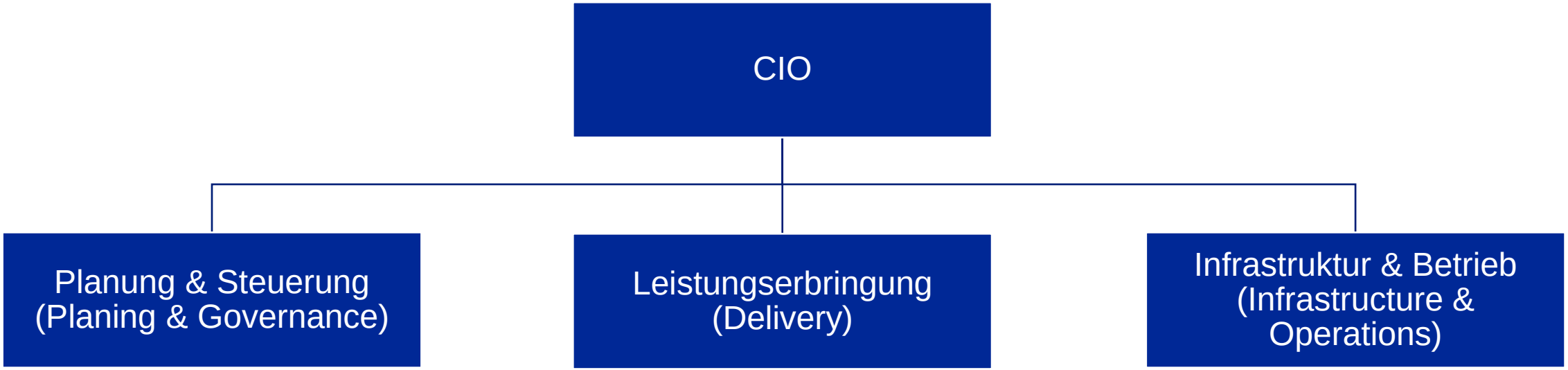
- Unternehmen mit ca. 6.000 Mitarbeitenden
- Vertreten in 20 Ländern mit insgesamt 28 eigenständigen Gesellschaften
- In den Gesellschaften sind vereinheitlichte Prozesse vorhanden

Diskutieren Sie im „Paar“ / Team mögliche IT-Organisations-formen für das Unternehmen. Gehen Sie auf Vor-, Nachteile und Konsequenzen ein.



PROZESSOPTIMIERTE IT-ORGANISATION
(REFERENZVORSCHLAG NACH GARTNER 2021)

Whitepaper in ILIAS



- Sicherheit & Risiko-Mgmt.
- Budget & Berichtswesen
- Projekt & Portfolio Mgmt.
- Zentrale Beschaffung und Lieferantenmanagement
- Standards & Vorgaben
- IT-Perfomance Mgmt.

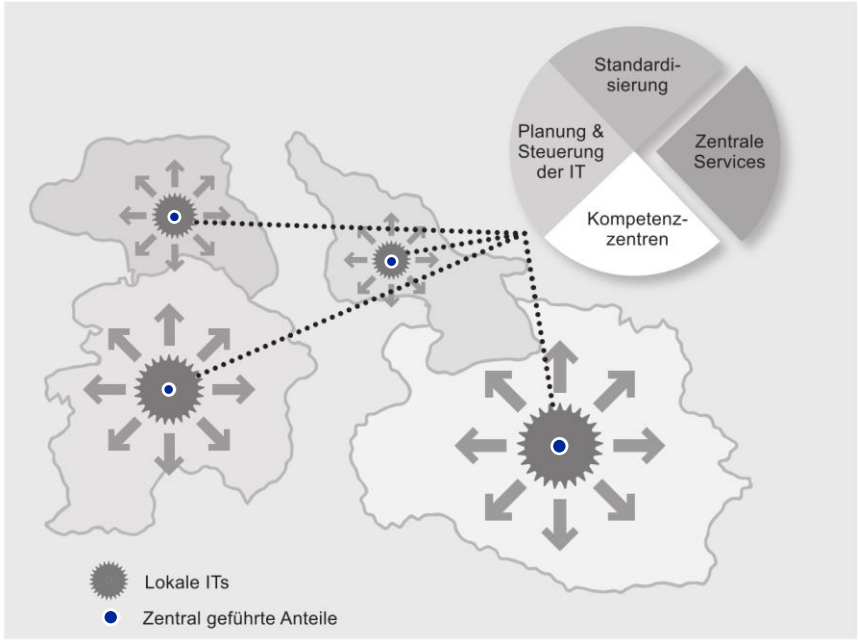
- [Projektmanagement]
- Geschäftsanalyse
- Solution Architektur
- Qualitätssicherung
- Software-Entwicklung
- Implementierung / Konfiguration

- Infrastruktur
  - Server & Speicher (Storage)
  - Netzwerk & Sicherheit
- Betrieb
  - Endanwender Support
  - Datenbanken
  - Tools & Anwendungen

GLOBALISIERUNG IN DER (KONZERN-)IT
„THINK GLOBAL – ACT LOCAL“

Globalisierungstendenz in globalen Konzernen
- Wandel von einer zentralen IT zu einer globalen IT
- Ziel: Nutzung der unterschiedlichen Kompetenzen, regionalen Vorteilen und kulturellen Besonderheiten

Herausforderungen
- Schaffung von organisatorischen und technischen Strukturen, die Zusammenarbeit und Teilung von Wissen fördert
- IT-Governance über alle lokalen IT-Einheiten zentralisiert
- Teams müssen erforderliche Skills haben. Interkulturell Kompetenzen, Teamfähigkeit, Reisebereitschaft.
- Weltweit einheitliche Methoden und Werkzeuge für alle Kernaktivitäten (Projektmanagement, EAM, usw.)
- Etablierung einer globalen Führung und Schaffung eines Anreizsystems (Zielvereinbarungen)



HOCHSCHULE HEILBRONN

› SOURCING MODELLE

IT-SOURCING

Das IT-Sourcing befasst sich mit der Fragestellung, welche IT-Tätigkeiten aus wirtschaftlicher Betrachtung **intern oder extern** sowie im **Inland oder Ausland** ausgeführt werden.

MOTIVE FÜR „BESCHAFFUNG AM MARKT“

- **Kurzfristig erforderliche Kapazitäten** werden möglicherweise nicht auf Dauer benötigt. Beispiel: Einführung einer neuen ERP-Lösung. Nach der Einführungsphase wird IT-Personal zwar für den Betrieb bzw. die Weiterentwicklung der Losung benötigt, aber weniger für die Entwicklung & das Customizing.
- Die rasche technologische Entwicklung lässt immer wieder **neue Tätigkeitsfelder** entstehen, bei denen die Personalressourcen (zunächst) knapp sind, sodass auf externe Ressourcen zurückgegriffen wird. Beispiel: Einführung von KI-Modellen.
- Sehr **spezialisierte IT-Aufgaben** können oftmals von Fachfirmen professioneller und wirtschaftlicher erbracht werden. Beispiel: Betrieb eines Security Operation Centers.
- Durch die Bündelung von Leistungen bei einem Service-Provider entstehen **wirtschaftliche Vorteile** durch Skaleneffekte. Beispiel: Cloudnutzung bei Hyperscaler
- Um innerbetriebliche Fachkompetenz im IT-Bereich aufzubauen, sind in der Regel externe **Schulungs- und/oder Beratungsleistungen** erforderlich.
- Im Rahmen von IT-Projekten werden oft unternehmenspolitisch **heikle Veränder-ungen** vorgenommen, die mit Unterstützung durch namhafte Beratungsunternehmen leichter durchsetzbar sind als ausschließlich intern erarbeitete Vorschläge.

BEGRIFFSDEFINITION

Outsourcing

Outsourcing bedeutet Auslagerung und bezeichnet die Abgabe von Aufgaben in Unternehmen an externe Dienstleister. Dies können auch ganze Abteilungen sein. Outsourcing ist eine Art des Fremdbezugs zu einer bis dahin intern erfolgten Leistung.

Subform: Outtasking

Im Vergleich zum klassischen Outsourcing, werden beim Outtasking lediglich einzelne Aufgaben („Tasks“) an einen externen Dienstleister vergeben. Dadurch behält der Auftraggeber die Kontrolle über z.B. IT-Infrastruktur, Prozesse und Personal.

Subform: Business Process Outsourcing

In bestimmten Fällen werden gesamte Geschäftsprozesse ausgelagert, was zu einem Business Process Outsourcing (BPO) führt. Diese Praxis ist nicht spezifisch für IT, da auch Buchhaltung oder Rekrutierung beispielsweise ausgelagert werden können.

BEGRIFFSDEFINITION

Insourcing	Insourcing (auch Backsourcing) bezeichnet die strategische Wiedereingliederung ausgelagerter Prozesse, Tätigkeiten oder Funktionen in eine Organisation. Dies setzt voraus, dass diese Prozesse zuvor ausgelagert wurden. Gelegentlich können auch zusätzliche Aufgaben integriert werden, um die Wertschöpfung zu erweitern oder das interne Tätigkeitsfeld zu stärken.
Offshoring	Offshoring ist die Praxis, Geschäftsprozesse oder Dienstleistungen in ausländische Länder zu verlagern, um Kosten zu senken oder Fachkräfte zu erreichen. **Subform: Nearshoring** Verlagerung in Länder mit regionaler Nähe (z.B. innerhalb von Europa wie Polen, Rumänien oder Bulgarien), um rechtliche und kulturelle Vorteile zu nutzen. **Subform: Farshoring** Verlagerung in Länder mit geringen Personalkosten und guter Personalverfügbarkeit (z.B. in Asien wie Indien oder Philippinen), um wirtschaftliche Vorteile zu nutzen.

GLOBALES SOURCING

Kriterien	Indien	Philippinen	China	Russland	Kanada	Irland
Steuerliche Vorteile	●	◐	○	○	◐	●
Verfügbarkeit von relevantem Fachwissen	●	◐	◐	○	◐	○
Infrastruktur	◐	●	●	○	●	●
Ausbildungssystem	●	◐	●	●	●	●
Kostenvorteile	●	●	●	●	◐	○
Servicequalität	●	●	○	○	●	●
Kultureller Fit	◐	●	○	○	●	●
Zeitunterschied	○	○	○	◐	●	●
Englischkenntnisse	●	●	○	○	●	●

Nutzung der Stärken und Vorteile der Regionen

SOURCING-MODELL

Welche IT-Leistung kann bzw. soll ein Unternehmen selbst erbringen
bzw. welche Leistungen sollen eingekauft werden?

Vorteile und Chancen

- IT-Abteilung kann Fertigungstiefe variieren
- Auf Nachfrageschwankungen flexibel reagieren
- Qualitäts- und Preisvorteile einkaufen
- Einkauf von speziellen, neuen oder selten gebrauchten Skills
- Einbindung des Lieferanten zur zusätzlichen Steigerung des Wertbeitrages

Nachteile und Risiken

- Abhängigkeitsverhältnis gegenüber einem Anbieter
- Risiko der Verschlechterung der Qualität
- Kontrollverlust (z.B. Datensicherheit)
- Verlust von Expertise und Wissen über die Prozesse und IT-Tätigkeiten
- Erhöhter Kommunikations- und Abstimmungs-aufwand (→ Transaktionskosten)
- Rückgang der Zufriedenheit und Motivation der Mitarbeitenden

SOURCING-MODELL

Welche IT-Leistung kann bzw. soll ein Unternehmen selbst erbringen bzw. welche Leistungen sollen eingekauft werden?

Basis für die Sourcing-Entscheidung

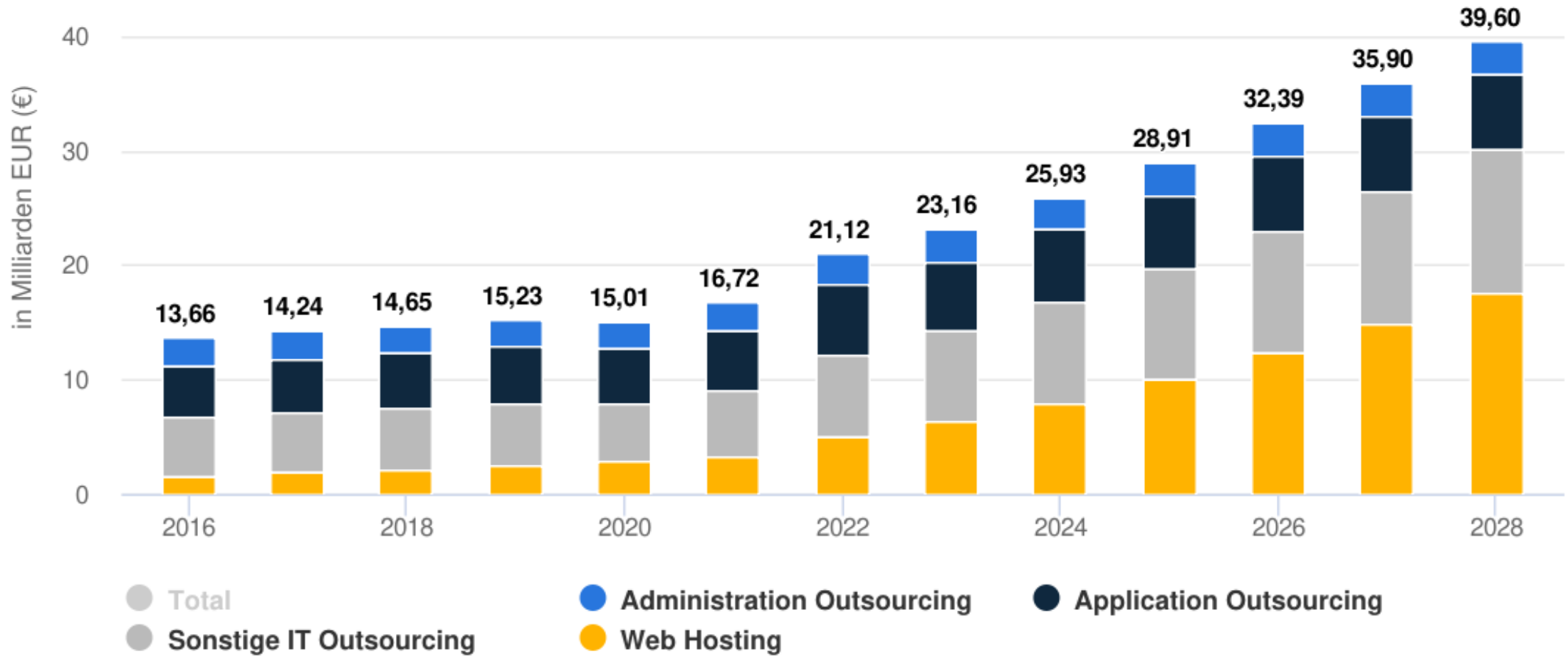
- Strategische Positionierung der IT und das Leistungspotenzial der IT
- Unterscheidung von strategischen und nichtstrategischen Elementen (Commodity).
- Kernkompetenz im Unternehmen vs. Commodity außerhalb des Unternehmens
- Aber bei Entscheidung Transaktionskosten mit betrachten!
  - Kosten für Auftragsvergabe (Ausschreibung, Angebote, Verträge)
  - Kosten für Transition & Transformation (T&T) Phase
  - Kosten für Koordination und Kontrolle
  - Mehraufwände bei Aufgabendefinition (z.B. Verlagerung auf Fachabteilungen)

Leistung	Partnerschaftsmodelle			Nutzen
Prozess-Verantwortung			Process Management	Prozessoptimierung
Anwendungen & Infrastruktur			Business Process Outsourcing Komplett-Outsourcing	Konzentration, Kosten-einsparung, Innovationszugang
Spezielle Lösungen			Business / IT Services	Optimierte Lösungen
Komponenten der Infrastruktur		Partielles Outsourcing		Leistungstransparenz, Kostenvorteile
Knowhow und Ressourcen	Professional Services Project Services			Skill- und Ressourcen-Vorteile
	kurzfristig	mittelfristig	langfristig	

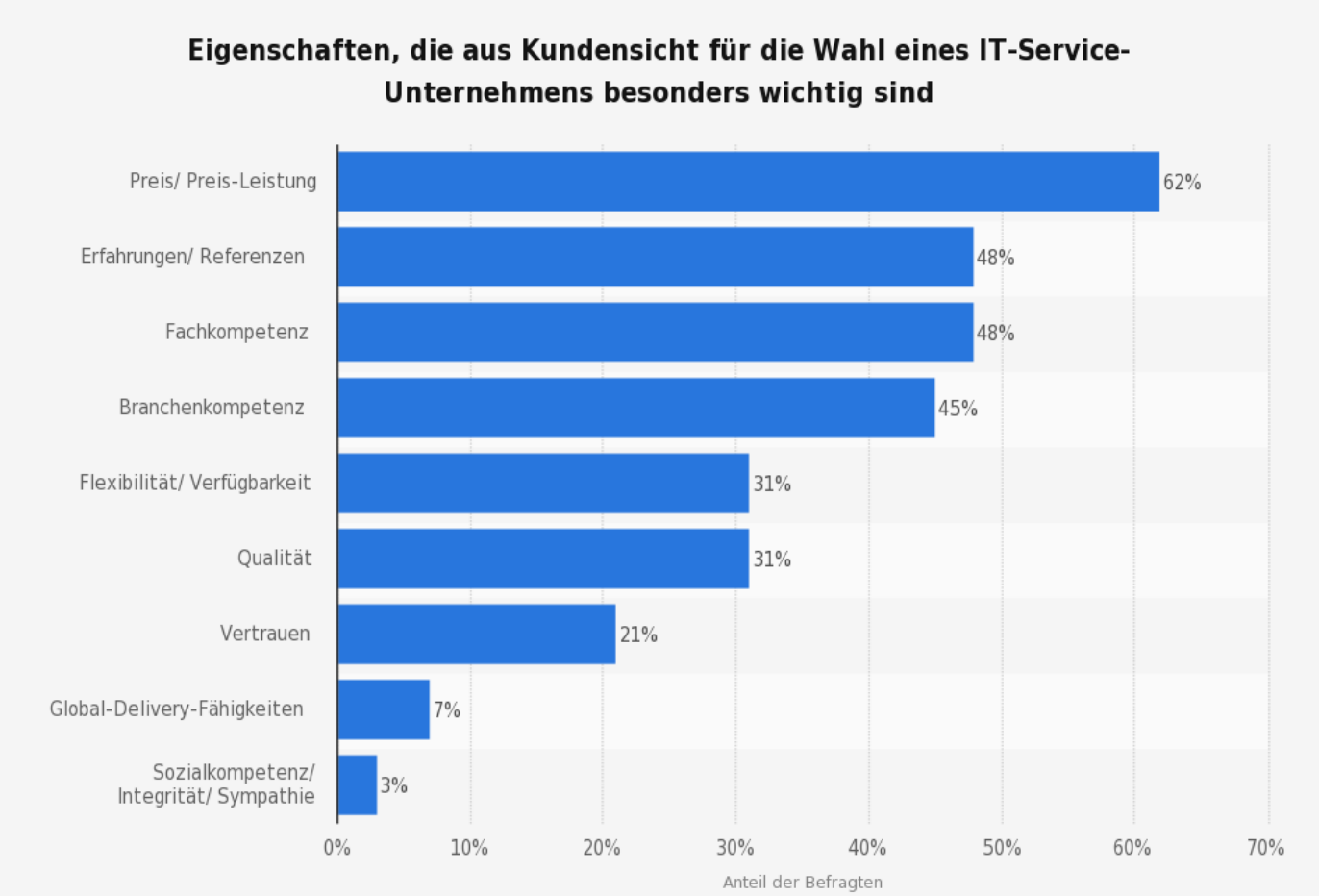
Optimierungsgrad

TREND: OUTSOURCING

UMSATZ MIT IT-OUTSOURCING IN DEUTSCHLAND IN MRD. EURO

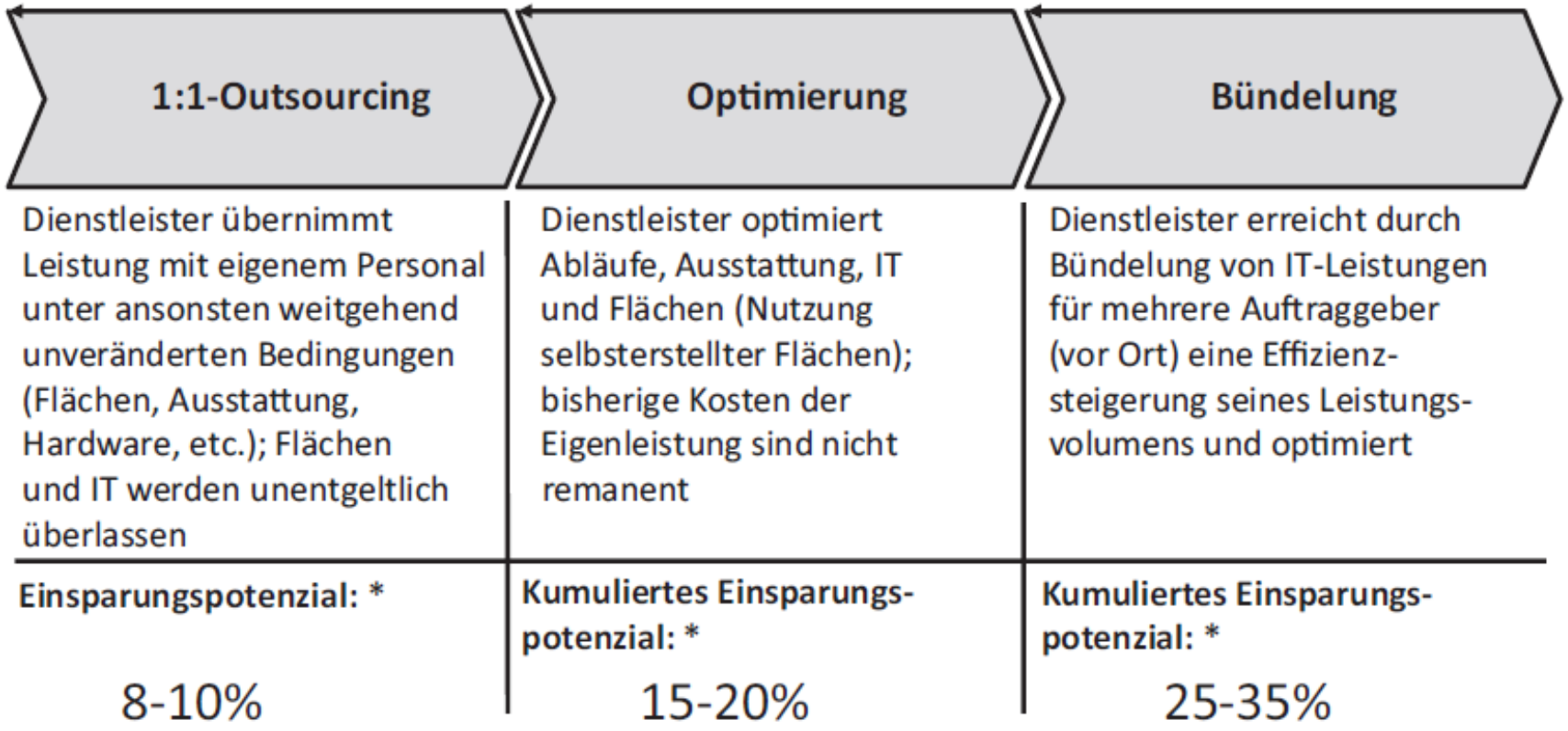


ENTSCHEIDUNGSGRUNDLAGE IT-SOURCING



Quelle: Statista / Lünendonk

OUTSOURCING UND DIE WIRKUNG AUF DIE KOSTEN



* bezogen auf das direkt beeinflussbare Volumen, Beispiel eines Industrieunternehmens

ANGEBOTSANFRAGEN

Im Zuge von Ausschreibungen im Outsourcing Kontext werden heute häufig folgende Begriffe verwendet:

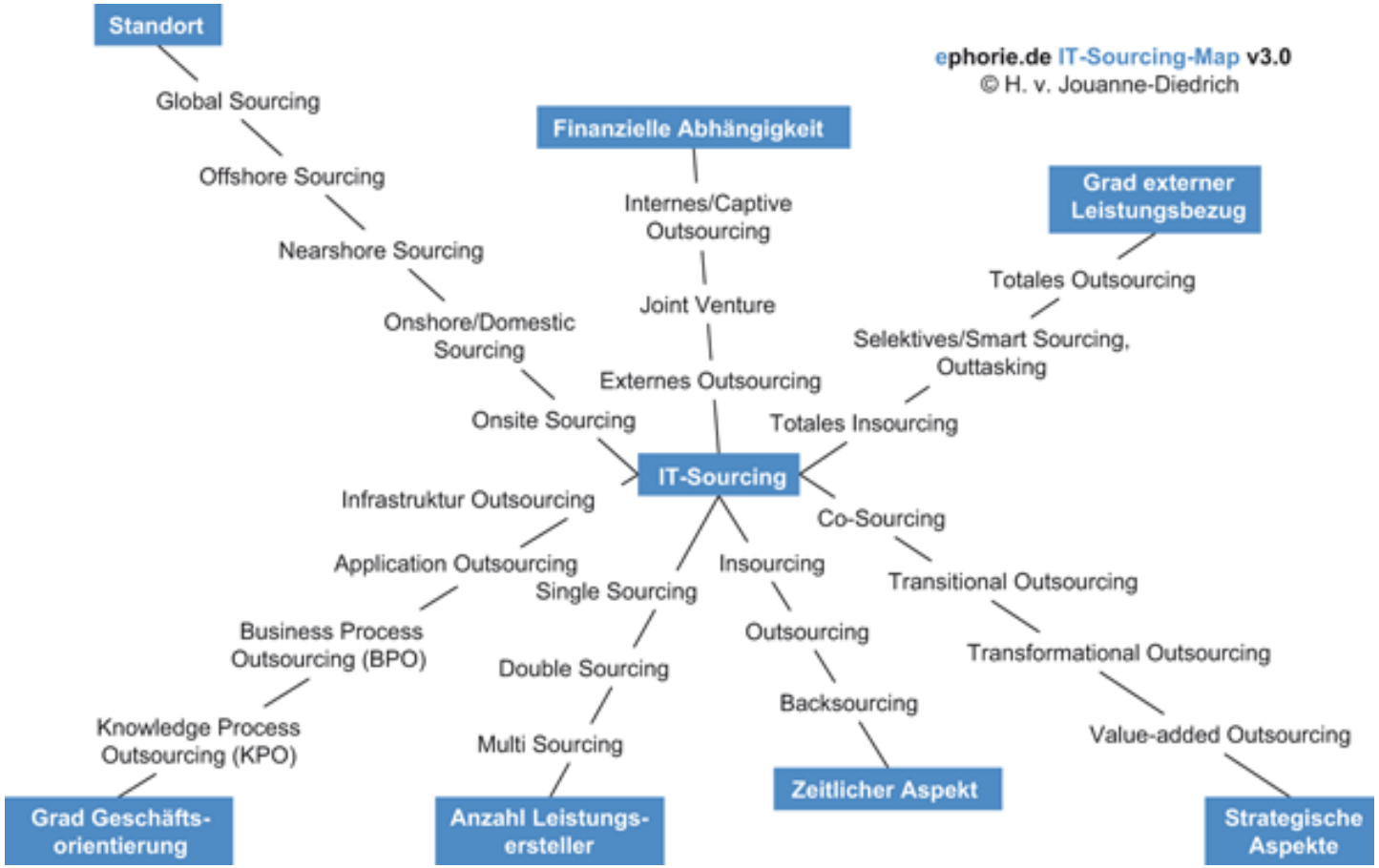
RFI Request for Information	Der Request for Information zählt zu der Vorauswahl eines potenziellen neuen Lieferanten oder einer Ausschreibung und beinhaltet meist die Informationseinholung über Produkte und Services, um zu klären, ob der Bedarf grundsätzlich erfüllt werden kann. Der RFI ist weniger formal und detailliert als der RFP oder der RFQ.
RFP Request for Proposal	Der Request for Proposal ist die schriftliche Aufforderung zur Angebotsangabe und erfolgt nach dem RFI. Im RFP sind alle Anforderungen des Auftraggebers detailliert dokumentiert. Eine Verpflichtung zur Annahme eines der Angebote besteht nicht.
RFQ Request for Quotation	Der Request for Quotation ist die Preisanfrage eines Auftraggebers, um Informationen über die Konditionen und einen möglichst präzisen Preis des potenziellen Lieferanten zu einem vorab beschriebenen Bedarf zu erfahren. Ein RFQ wird verwendet, wenn man bereits genau weiß, was man genau benötigt und wofür es verwendet wird.

GRUNDSÄTZE AM BEISPIEL

ANFORDERUNGEN GEMÄß FINMA-RS 08/7 „OUTSOURCING-BANKEN“

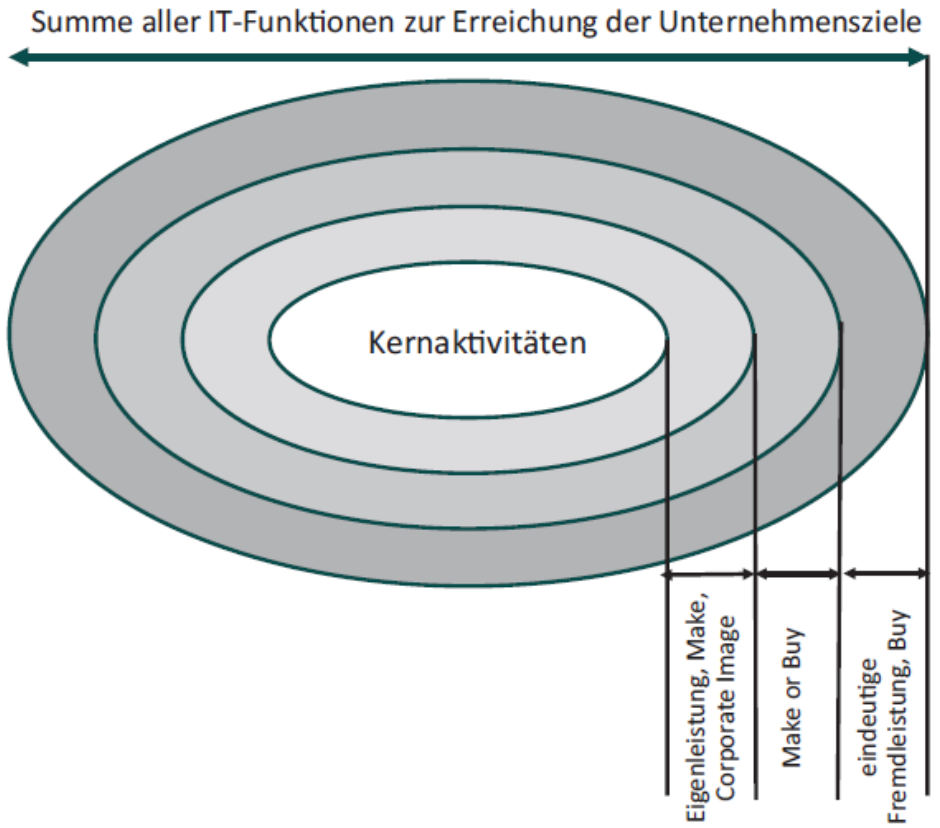
1. **Definition** des Outsourcing-Umfangs (was wurde ausgelagert?)
2. Sorgfältige **Auswahl, Anweisung und Überwachung** des Outsourcing- Partners
3. **Verantwortung** (die Bank bleibt verantwortlich und haftbar)
4. **Sicherheit** (Sicherheitsfragen werden angemessen angegangen)
5. Bankgeheimnis und Datenschutz (**Vertraulichkeit** gemäß Schweizer Gesetze)
6. **Kundenorientierung** (Kunden müssen über das Outsourcing informiert sein)
7. **Kontrolle und Überwachung** (interne und externe Prüfer müssen über alle Aktivitäten informiert werden)
8. Auslagerung in ein ausländisches Land (**spezielle Bedingungen** müssen erfüllt werden)
9. **Vertrag** (schriftlicher Vertrag mit klaren Bedingungen für die Gültigkeit erforderlich)

IT-SOURCING MAP NACH JOUANNE-DIEDRICH



SOURCING MODELL – STRATEGIE
VORGEHEN

- Festlegung der Sourcing Strategie wird auf Basis der Analyse und Bewertung des Leistungspotentials der IT vorgenommen werden.
- Alle operative und strategische IT Management Aktivitäten werden möglichen Insourcing-, Outsourcing-, Offshoring-Initiativen gegenübergestellt und zugeordnet
- Ein transparenter Kriterienkatalog dient als Entscheidungsgrundlage (u.a. Chancen, Risiken, strategische Relevanz, Austauschbarkeit, Lieferantenvielfalt, Qualitätsverbesserungen, Skalen-effekte, etc.)



SOURCING MODELL – STRATEGIE
WESENTLICHE EMPFEHLUNGEN

Wesentliche Empfehlungen zur Sourcing Strategie

- Ermittlung des Leistungspotenzials sowie die Kerneigenleistungsfähigkeit
- Sourcing-Strategie im Rahmen der IT-Strategie formulieren
- Tendenziell gilt:
  - → **Kernkompetenzen** sollten im Unternehmen bleiben (u.a. EAM, Geschäftsprozessmanagement, Business Capability Management, etc.)
  - → Ressourcen bleiben nur im Unternehmen, wenn Sie **bleibende Werte** schaffen
  - → Wenn es keinen Anbieter für die Leistung im Markt gibt, dann ist der Aufwand für die Analyse umsonst

HOCHSCHULE HEILBRONN

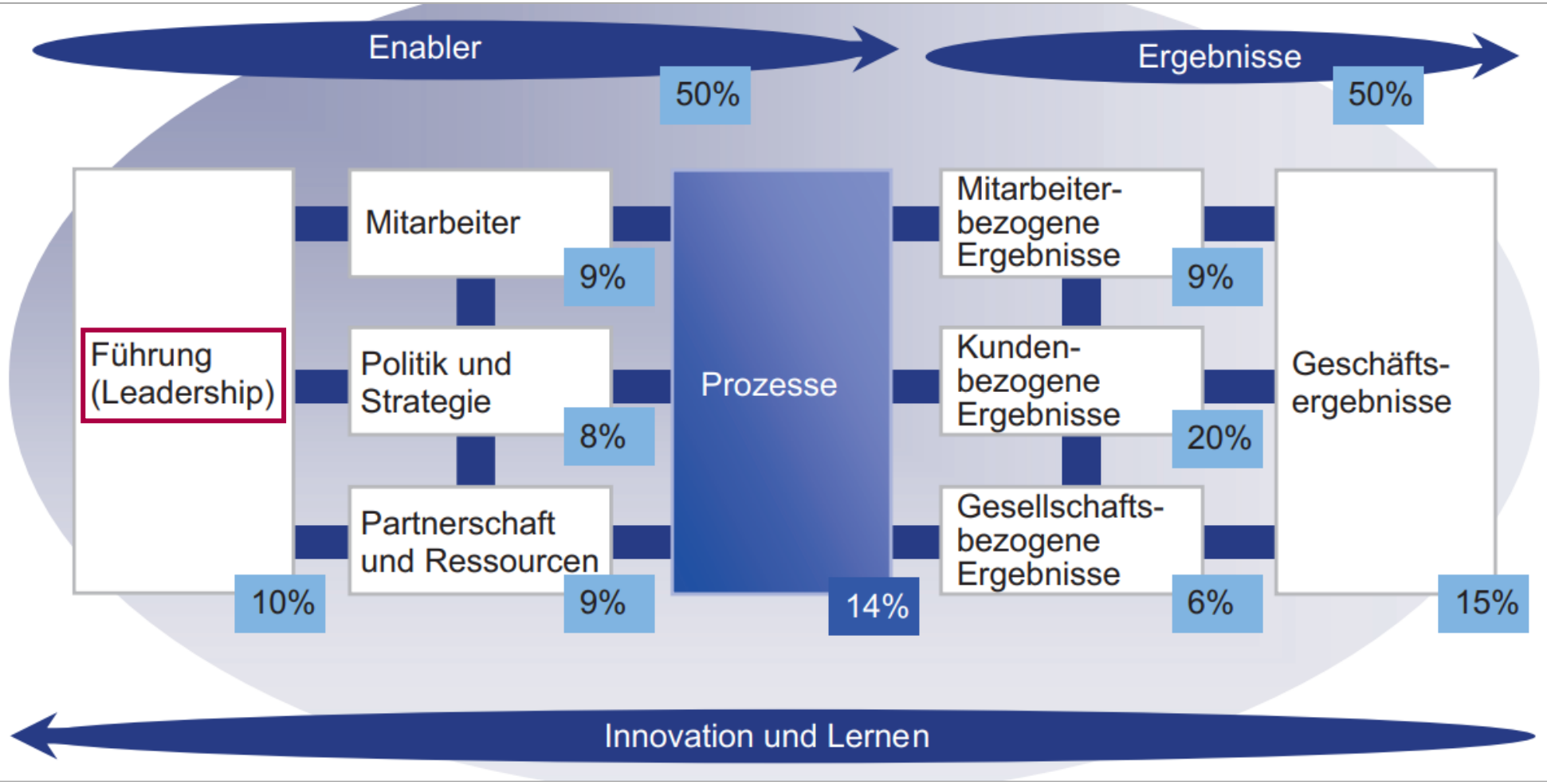
› PERSONAL & LEADERSHIP

WARUM BENÖTIGT ES LEADERSHIP?

- Aufgaben im IT-Bereich können nur dann erfolgreich gelöst werden, wenn IT-Fachkräfte mit den notwendigen **Kompetenzen und Qualifikationen** vorhanden sind
- Mitarbeitende im IT-Bereich müssen über ausreichende **Leistungs-bereitschaft** (nicht nur Leistungsfähigkeit) bzw. **Motivation** verfügen → förderliche Rahmenbedingungen
- IT bedeutet auch kontinuierliche **Veränderung**: Mitarbeiter müssen aktiv mitgenommen werden und Änderungen durchgesetzt werden
- Sicherstellung einer hohe **Ergebnisqualität** der Arbeiten in IT-Prozessen und IT-Projekten wird unter Beachtung wichtiger personeller **Erfolgs- und Qualitätsfaktoren**

ZUSAMMENHANG LEADERSHIP & ARBEITSERGEBNISSE

EUROPEAN FOUNDATION FOR QUALITY MANAGEMENT (EFQM)



ZIELE, HERAUSFORDERUNGEN UND HANDLUNGSNOTWENDIGKEITEN FÜR DAS PERSONALMANAGEMENT

IT-Führungskräfte verfolgen herausfordernde Ziele…

- IT-Vision / IT-Mission klären
- ROI der IT steigern
- Mitarbeiter-Produktivität erhöhen
- Kundenorientierung erhöhen Prozesse verbessern
- Teams zum Erfolg bringen
- Nachhaltige Strategien erarbeiten und umsetzen
- kompetente Mitarbeiter gewinnen und fördern
- IT-Fachkräfte mit hoher Kompetenz binden
- motivierte Mitarbeiter einsetzen können („great place to work“)

… und brauchen dazu immer andere Mitstreiter

Abwägen, entscheiden, begründen, …

Informieren, delegieren, beurteilen, …

Integrieren, überzeugen, vorleben, Vorbild sein, …

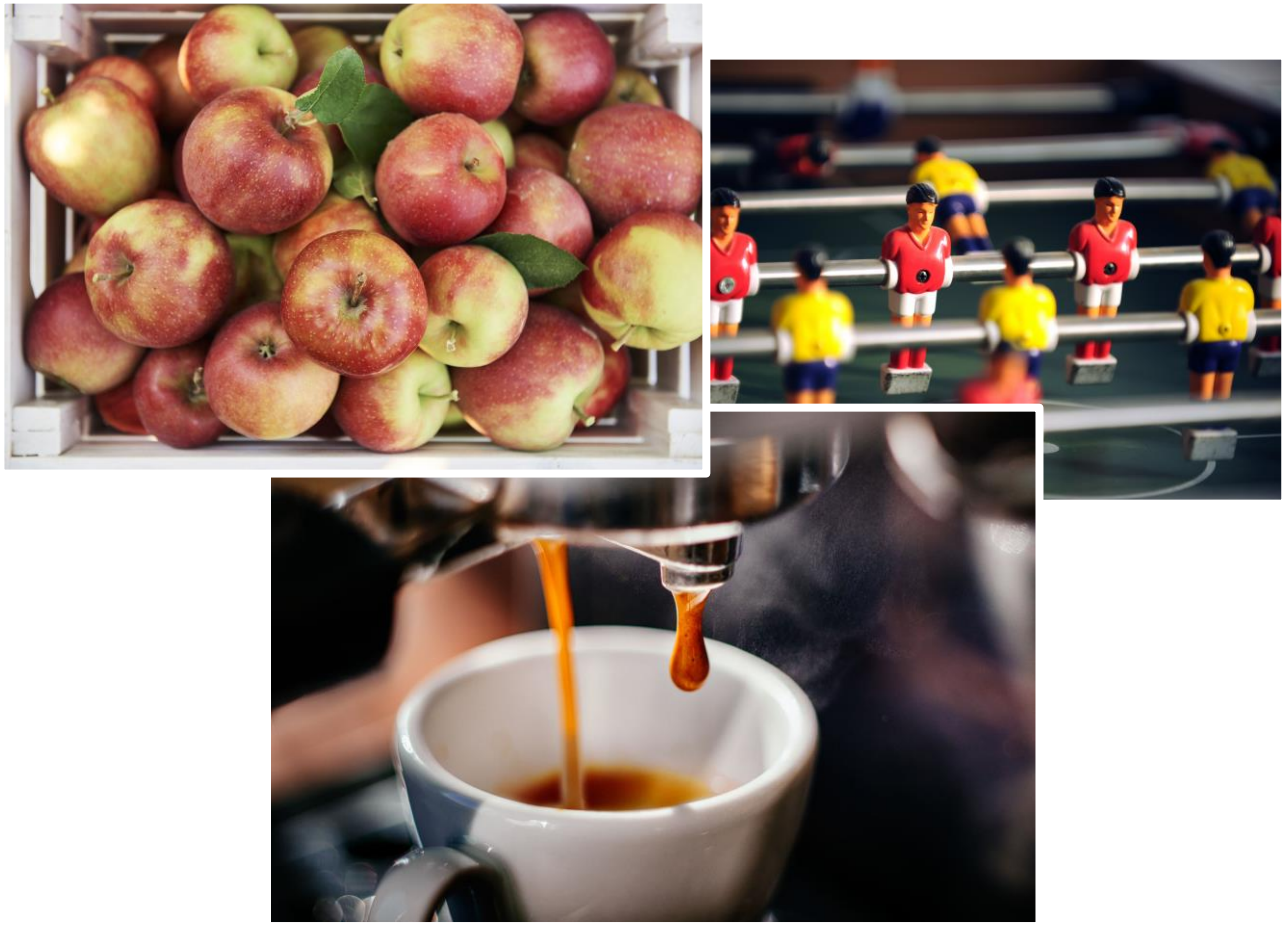
Zuhören, ernst nehmen, schützen, motivieren, aufpäppeln, …

Spielführer sein, Mentor sein, Coach sein, Mitspieler sein, …

Situationen / Herausforderungen

- veränderte Anforderungen an das IT-Fachpersonal (zum Beispiel durch digitale Transformation etc.)
- starke Personalfluktuationen im IT-Bereich
- hohe Komplexität der Systemlandschaft
- ...

MITARBEITERMOTIVATION HAT NICHTS MIT OBSTKÖRBEN ZU TUN, ODER?



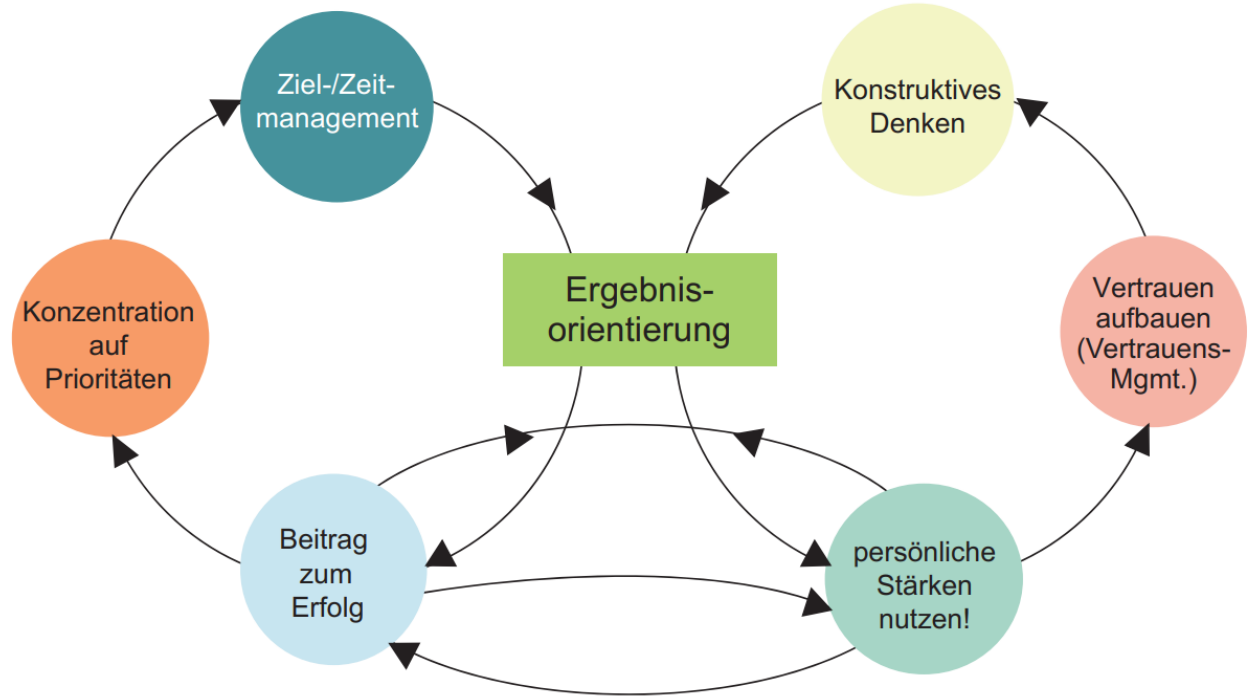
Wie sehen Sie das?

FÜHRUNGSGRUNDSÄTZE

Die einer IT-Führungskraft übertragene Autorität muss mit fachlicher, methodischer und sozialer Kompetenz ausgefüllt werden.

Führungsgrundsätze können ein erfolgreiches Handeln in Führungs-situationen ermöglichen & gewährleisten:

- Vertrauen aufbauen
- Begeisterung wecken
- Wertschätzung den Mitarbeitern entgegenbringen
- Positive Zukunftsperspektiven eröffnen



AUFGABEN IM PERSONALMANAGEMENT

Strategische IT-Personalplanung

- Personalbestandsanalyse
- Strategische Personalbedarfsfestlegung
- Abweichungsanalyse
- Entwicklung strategischer Handlungspläne
- Fortschrittskontrolle

IT-Personal-Recruiting

- Stellen- / Tätigkeitsbeschreibung
- Initiierung des Einstellungsprozesses
- Durchführung von Bewerbungsgesprächen
- Personalauswahl
- Unterstützung des Onboarding-Prozesses

Personalentwicklung

- Feststellung von Aus- und Weiterbildungsfeldern (Kenntnisse, Fähigkeiten und Verhalten)
- Initiierung, Entwicklung, Förderung und Durchführung von Maßnahmen
- Individuelle Personalentwicklungskonzepte erstellen
- Rahmenbedingungen für das Lernen schaffen

Change-Management

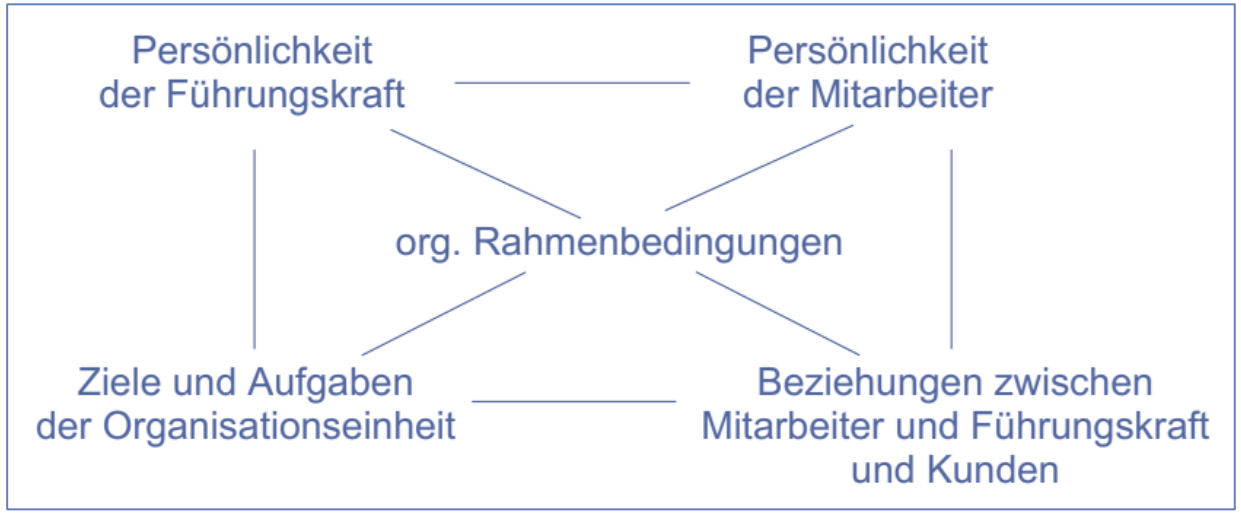
- Identifikation von notwendigen Change-Management Maßnahmen
- Mitwirkung und Unterstützung bei organisatorischen Veränderungsprozessen

DIREKTE FÜHRUNGSAUFGABEN

PERSONALFÜHRUNG

Personalführung kann in der heutigen Zeit nur dann erfolgreich sein, wenn ein die Persönlichkeit **respektierendes Menschenbild** und die **Wert-schätzung** der Mitarbeiter Handlungsmaßstab für die IT-Führungskraft ist.

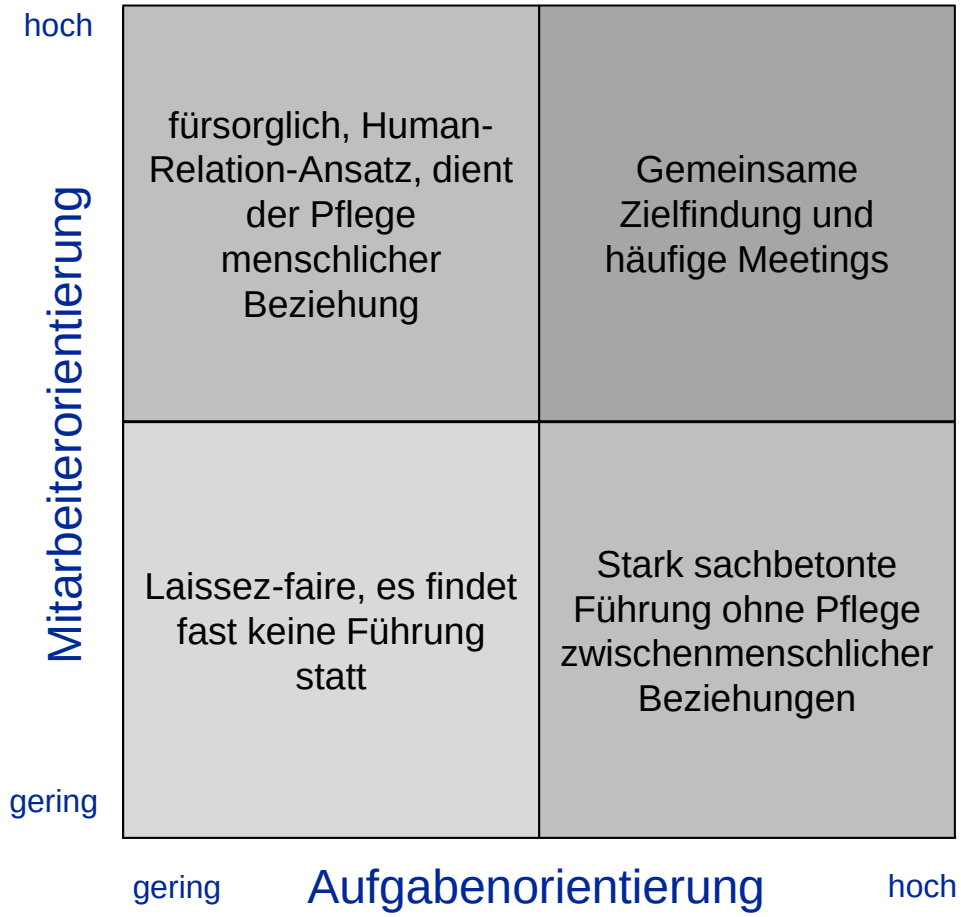
Mit einem **partnerschaftlich-dialogischen Führungskonzept** kann dem Selbstverständnis gut ausgebildeter, mündiger IT-Mitarbeiterinnen und IT-Mitarbeiter entsprochen werden.



IT-Führungspersönlichkeiten müssen in der Zukunft ihre **Macht teilen** und „loslassen können“, ja sie müssen ihren anvertrauten Mitarbeiterinnen und Mitarbeitern mehr **zutrauen**.

Persönliches **Charisma** und **Glaubwürdigkeit** sowie **Offenheit** der Führenden werden mitunter zu entscheidenden Prämissen für den Führungserfolg

PERSONALFÜHRUNG



Es keinen generell „richtigen“ Führungsstil. Es gibt nur einen subjektiv/ situativ richtigen, authentischen Stil, der permanent weiterentwickelt werden sollte:

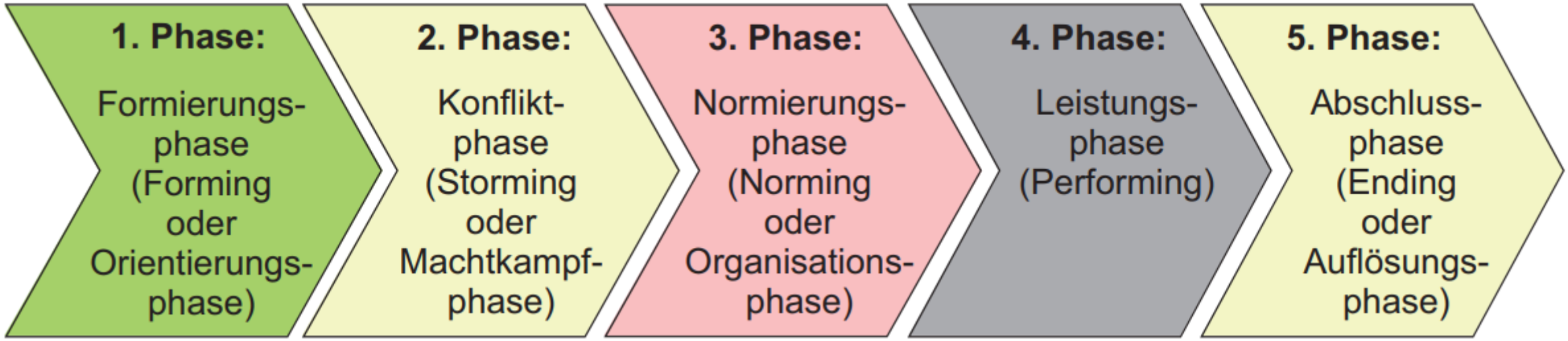
- wertschätzender Führungsstil
- fördernder Führungsstil
- anspornender Führungsstil
- integrierender Führungsstil
- ermutigender Führungsstil
- bremsender Führungsstil

INSTRUMENTE DER MITARBEITERFÜHRUNG

- Zielvereinbarung (Führungsziele, fachliche Ziele, persönliche Ziele)
- Anlassbezogene Mitarbeitergespräche
- Institutionalisierte Mitarbeitergespräche (z.B. Jahresfeedback, Zielvereinbarung)
- Konfliktmanagement (Erkennen, analysieren, konstruktiv bearbeiten)
- Teambuilding & Verhaltenkodex

TEAMENTWICKLUNG

Der Mensch für sich allein vermag gar wenig und ist ein verlassener Robinson; nur in der Gemeinschaft mit den andern ist und vermag er viel. *(Arthur Schopenhauer)*



› COMPLIANCE, RECHTSFRAGEN & NORMUNG

Compliance [Regelkonformität]

Compliance liegt vor, wenn alle für das Unternehmen verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.

Dort, wo ein Unternehmen nicht compliant ist, liegt ein Compliance-Verstoß, häufig auch als „Non-Compliance“ bezeichnet, vor.

Der Compliance-Prozess umfasst die Identifikation, Umsetzung, Dokumentation und Überwachung von internen und externen Vorgaben.

PROMINENTE BEISPIELE VON VERSTÖSSEN

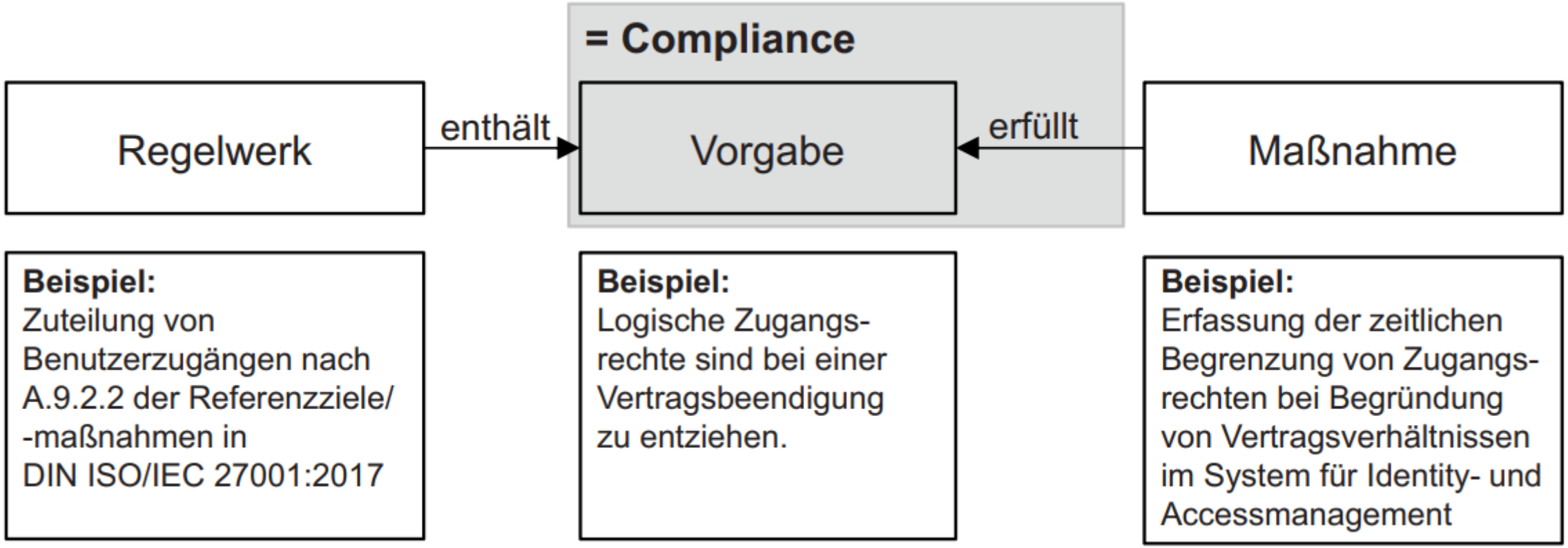
IN DER WIRTSCHAFTSPRESSE FINDEN SICH REGELMÄßIG BEISPIELE

Kartellstrafen
Das Bundeskartellamt hat 2022 rund 24 Mio. Euro Bußgeld gegen insgesamt 20 Unternehmen und 7 natürliche Personen verhängt.

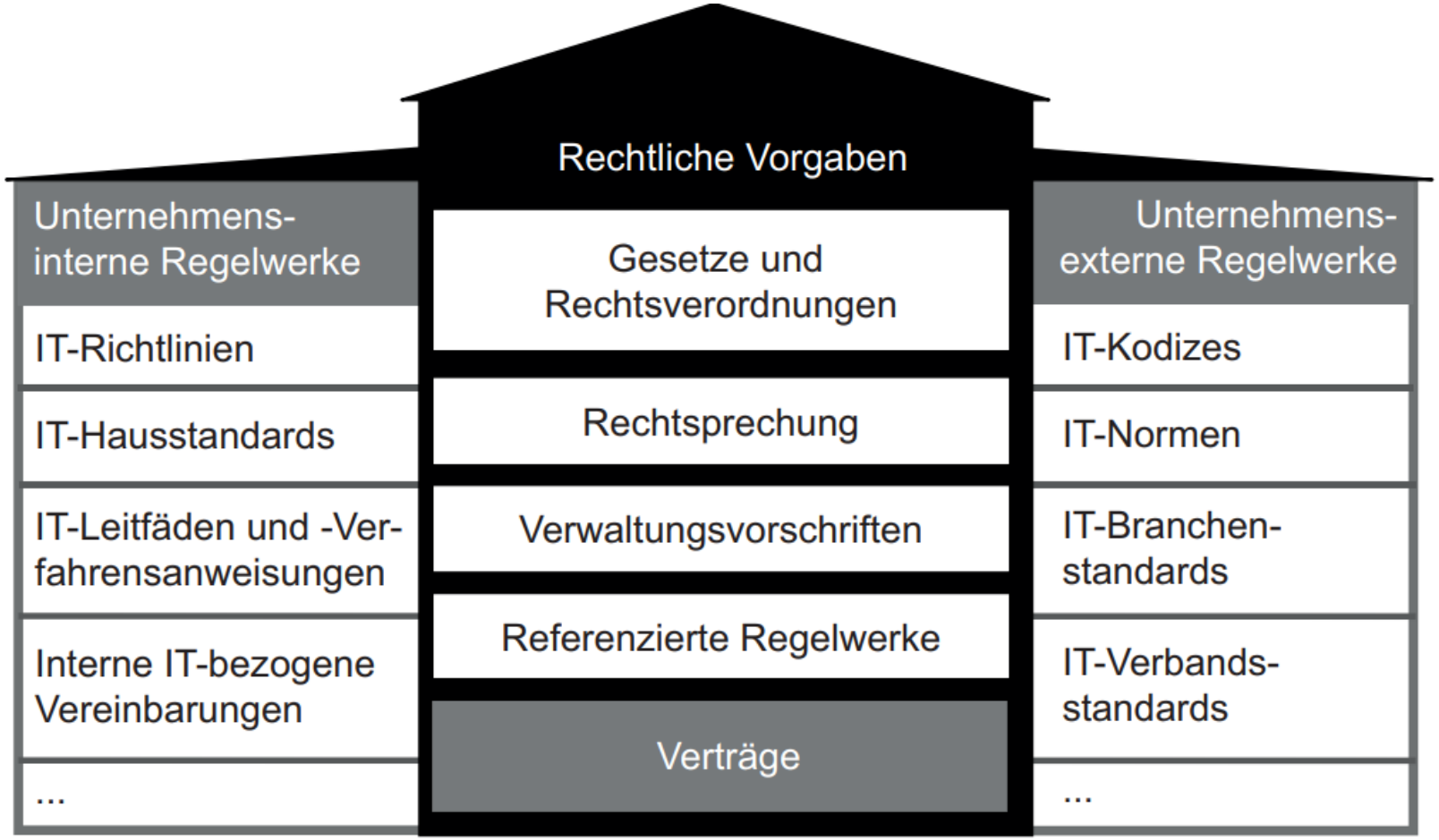
Dieselskandal
Seit 2015 der Skandal um „Schummelsoftware“ zur Manipulation von Abgaswerten Aufmerksamkeit erfahren. VW wurde bis vor den BGH verklagt.

Wirecard-Skandal
Anklage des Managements des Finanzdienstleisters nach bekanntwerden des Betrugs (u.a. Fälschung von Bilanzen und Geldwäsche)

IT-COMPLIANCE
ERFÜLLUNG VON VORGABEN



HOUSE OF COMPLIANCE



RECHTLICHE VORGABEN (AUSZUG)

Bundesdatenschutzgesetz (BDSG) Datenschutzgrundverordnung (DSGVO) Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)	Umgang mit personenbezogen Daten
Sarbanes Oxley Act (SOX) Gesetz zur Kontrolle und Transparenz (KonTraG)	Risikomanagement
Bürgerliches Gesetzbuch (BGB) Handelsgesetzbuch (HGB) Gesetz gegen den unlauteren Wettbewerb (UWG)	Wirtschaftsgesetze
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik IT-Sicherheitsgesetz i.V.m. KRITIS-Verordnung Telemediengesetz (TMG)	IT-Gesetze
Energiewirtschaftsgesetz (EnWG) Good x Practices (GxP, z.B. Good Manufacturing Practice)	Branchengesetze

RECHTLICHE VORGABEN

Rechtsprechung
Zu den rechtlichen Vorgaben zählt weiterhin die Rechtsprechung, die die Rechtsnormen auslegt und damit wesentlich deren Inhalt bestimmt.

Beispiel:
Das Oberlandesgericht Hamm stellte 2003 fest, dass eine Datensicherung täglich zu erfolgen hat, eine Vollsicherung mindestens einmal wöchentlich (Az. 13U133/03)

Verwaltungsvorschriften
Als Regelwerke relevant, die von den zuständigen (Aufsichts-) Behörden zur Interpretation und Ausführung der Rechtsnormen aufgestellt oder erklärtermaßen herangezogen werden.

Beispiel:
Vom Bundesministerium für Finanzen (BMF) als Verwaltungs-anweisung erlassenen „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern“ GoBD

In Bezug genommen Regelwerke
Durch ausdrücklichen Verweis auf öffentliche oder privatwirtschaftliche Regelwerke (z.B. DIN / ISO Normen) erhalten diese die gleiche Bedeutung wie Rechtsnormen

Beispiel:
Die von der BaFin herausgegebene MaRisk verweist auf den BSI-Grundschutz als auch auf die Normenreihe ISO/IEC 2700x.

Norm

Eine Norm ist ein Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für die Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird.

Akteure: Deutsche Institut für Normung (DIN), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), Verband der Elektrotechnik, Elektronik, Informationstechnik (VDE)

HOCHSCHULE HEILBRONN

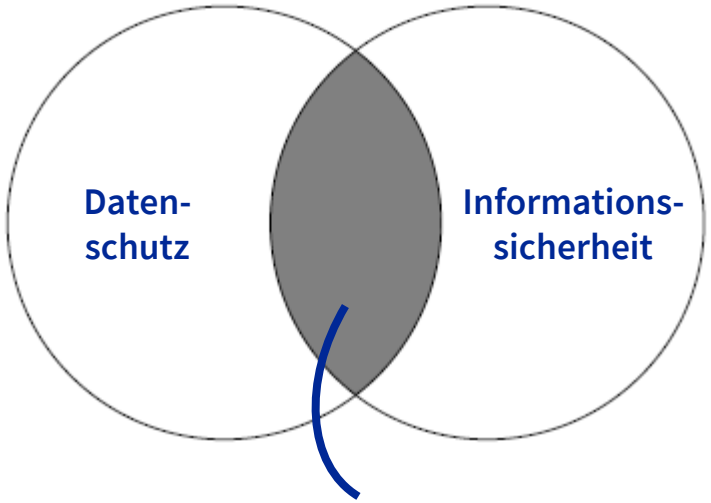
› DATENSICHERHEIT UND DATENSCHUTZ

DATENSCHUTZ VS. DATEN-/INFORMATIONSSICHERHEIT

Datenschutz

Datenschutz beschreibt den Schutz vor der **missbräuchlichen Verarbeitung** personenbezogener Daten sowie den Schutz des **Rechts auf informationelle Selbstbestimmung.**

„Legislative“
Gesetzgebung zum Schutz der informationellen Selbstbestimmung



Informationssicherheit, die zur Gewährleistung des Datenschatzes erforderlich ist

Daten- / Informationssicherheit

Die Datensicherheit bezieht sich dagegen auf den Schutz aller Informationen (und nicht nur personenbezogener Daten) **vor unbefugtem Zugriff, vor Korruption oder Diebstahl.**

„Exekutive“
Technische Maßnahmen zum Schutz der Daten

GRUNDSÄTZE DER DSGVO (§5)

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
2. Zweckbindung (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)
3. Datenminimierung („dem Zweck angemessen und erheblich sowie auf das […] notwendige Maß beschränkt“)
4. Richtigkeit („es sind alle angemessenen Maßnahmen zu treffen, damit [unrichtige] personenbezogene Daten unverzüglich gelöscht oder berichtigt werden“)
5. Speicherbegrenzung (Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es […] erforderlich ist“)
6. Integrität und Vertraulichkeit („angemessene Sicherheit der personenbezogenen Daten […], einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“)

VOM BDSG ZUR DSGVO

1. Einheitliche Regelung in allen Ländern der Europäischen Union zur Vereinheitlichung des Datenschutzniveaus
2. Datenverarbeitung nur mit Einwilligung
3. Höhere Fokus auf Datensicherheit
4. Höhere Bußgelder (bis zu 20 Mio. Euro)
5. Löschung von persönlichen Daten kann veranlasst werden

SCHUTZSTUFEN

Schutz-stufe	Personenbezogene Daten,	zum Beispiel	Schwere eines möglichen Schadens
A	die von den Betroffenen frei zugänglich gemacht wurden.	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite; frei zugängliche soziale Medien	geringfügig
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen").	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz").	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DS-GVO	substantiell
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	groß

GRUNDSCHUTZ

An welchen Stellen bestehen Gefahren für die Datensicherheit?

SCHUTZZIELE (CIA-TRIADE)

Integrität [Integrity]
Schutz vor unbefugter Manipulation von Informationen oder Daten

Verfügbarkeit [Availability]
Schutz von Beeinträchtigung der Funktionalität

Vertraulichkeit [Confidentality]
Schutz von unbefugter Informations-gewinnung

IT-GRUNDSCHUTZ-KOMPENDIUM

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- 1995 veröffentlicht als IT-Grundschutzhandbuch
- 2006 Trennung in methodischen Teil und Grundschutz Katalog
- 2017 Modernisierung zum IT-Grundschutz-Kompendium
- **Prozessbausteine:** Sie bilden organisatorische Domänen wie „Sicherheitsmanagement“ oder „Betrieb“ ab, die sich auf viele technische Objekte auswirken.
- **Systembausteine:** Mit den Systembausteinen werden technische Objekte wie „WebBrowser“ oder „Serverraum“ abgebildet.

BSI-STANDARDS

1. BSI-Standard 200 – 1: Managementsysteme für Informationssicherheit.
Der Standard definiert ein Managementsystem für Informationssicherheit (ISMS) und geht auf den Sicherheitsprozess und das Sicherheitskonzept ein. Dabei wird die Kompatibilität zum ISO-Standard 27001 gewahrt.

2. BSI-Standard 200 – 2: IT-Grundschutzmethodik.
Der Standard bildet die Basis für die Anwendung der IT-Grundschutzmethodik und für den Aufbau eines ISMS. Er konzentriert sich besonders auf den Sicherheitsprozess und die Erstellung einer Sicherheitskonzeption.

3. BSI-Standard 200 – 3: Risikomanagement.
Der Standard beschreibt die Durchführung der Risikoanalyse auf der Basis von IT-Grundschutz und die Behandlung von ermittelten Risiken. Dieses Vorgehen ist für Systeme mit höherem Schutzbedarf erforderlich.

ISO/IEC 27001:2013

Die Norm in ihrer aktuellen Fassung ISO/IEC 27001:2013 **– Information security management systems – Requirements** beschreibt die Anforderungen an ein ISMS und besitzt folgende Kernpunkte:

- **Führung** (Erstellung der Policy und Rollen / Verantwortlichkeiten)
- **Planung** (Etablierung Risikomanagementprozess)
- **Unterstützung** (Information-Security-Know-how durch Schulungen, etc.)
- **Betrieb** (Operative Durchführung des Information Security Management)
- **Leistungsbewertung** (Überwachung und Prüfung der Wirksamkeit bzw. Effektivität)
- **Verbesserung** (kontinuierlicher Verbesserungsprozess)

ZUSAMMENFASSUNG

- Grundbegriffe des IT-Managements
- Organisatorische Ausrichtung der IT-Abteilung
  - Vorteile der Organisatorischen Möglichkeiten
- Sourcing-Überlegungen
- Führungsaufgaben in der IT – Leadership und Stile
- Compliance und Anforderungen durch externe Regularien (House of Compliance)
- Auswirkungen der DSGVO zum Datenschutz
- Integrität, Verfügbarkeit und Vertraulichkeit als Schutzziele
- Normen und Gesetze wie ISO27001, SOX, GxP, KRITIS

HOCHSCHULE HEILBRONN

VIELEN DANK!

Bei Fragen kontaktieren Sie bitte:

Dr. Philipp Küller
Wirtschaftsinformatik
Philipp.kueller@hs-heilbronn.de