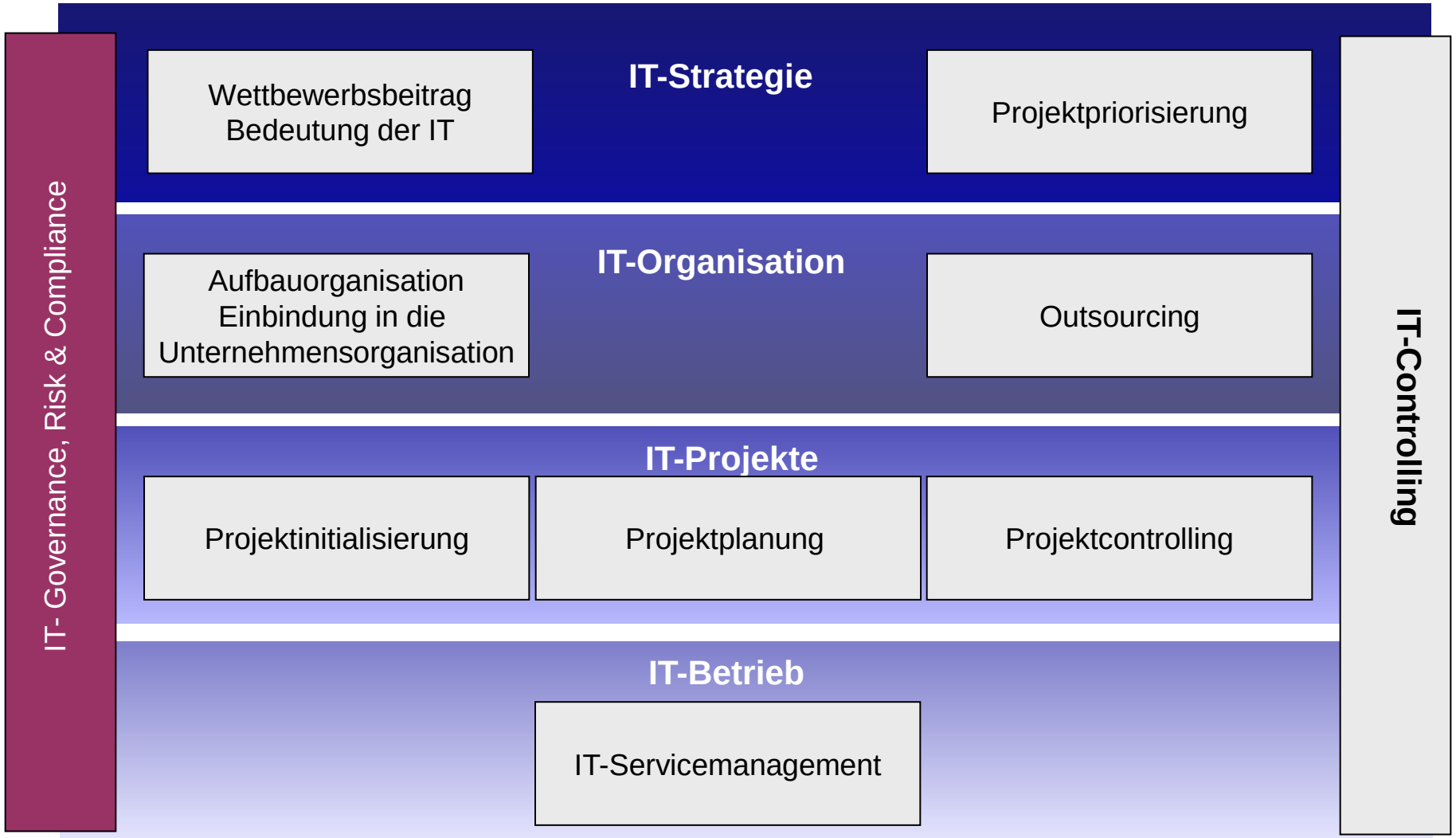
Inhalt

- Überblick
- IT-Strategie
- IT-Governance, Risikomanagement und Compliance
  - IT-Governance
  - IT-Risikomanagement
  - IT-Compliance
- IT-Organisation
- IT-Outsourcing
- IT-Servicemanagement

Themenüberblick



IT-Governance

“Die Verantwortung der Unternehmensführung und des Vorstands; besteht in der Führung, den organisatorischen Strukturen und Prozessen, die sicherstellen, dass die IT des Unternehmens die Strategien und Ziele des Unternehmens unterstützt und erweitert."

Quelle: https://www.isaca.org/resources/glossary

“IT-Governance bezeichnet den rechtlichen und faktischen Ordnungsrahmen für die Leitung, Organisation (prozessual wie aufbauorganisatorisch) und Überwachung der IT eines Unternehmens. Mit der IT-Governance soll sichergestellt werden, dass die Unternehmensziele durch den IT-Einsatz unterstützt und vorangetrieben werden.”

Quelle: Lackes, R., Siepermann, M. https://wirtschaftslexikon.gabler.de/definition/it-governance-53193

Governance vs. Management

Governance = Verkehrsregeln

- Straßenverkehrsordnung
- Polizei
- Strafzettel
- Ampeln
- Verkehrsschilder
- Fahrpläne
- …



Management = von A nach B kommen

- Startpunkt
- Bus, Bahn oder Auto nehmen?
- Autobahn oder Landstraße?
- S1 oder S3 ?
- Umsteigen in Altona oder Jungfernstieg
- Bei gelber Ampel wirklich halten?
- Ziel
- …

Quelle: in Anlehnung an Otto, B. / CC CDQ Universität St. Gallen

Referenzmodelle für das IT-Management (Auswahl)

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

IT-Governance	Unternehmens Architektur	IT-Projekt-management	IT Service-management	Software Engineering	IT-Sicherheit
COBIT	Zachman Framework	PMBOK	ITIL ISO/IEC 20000	CMMI-DEV	ISO/IEC 27000 Reihe
	TOGAF	IPMA ICB	Microsoft Operations Framework	Rational Unified Process	IT-Grundschutz
		PRINCE2	CMMI-SVC	SPICE	
…	…	…	…	…	…

COBIT: Überblick

- Ehemals „Control Objectives for Information and Related Technology“ mit Fokus auf Prüfungsanforderungen und IT-Risiken
- entwickelt von der Information Systems Audit and Control Association (ISACA)

COBIT ✓

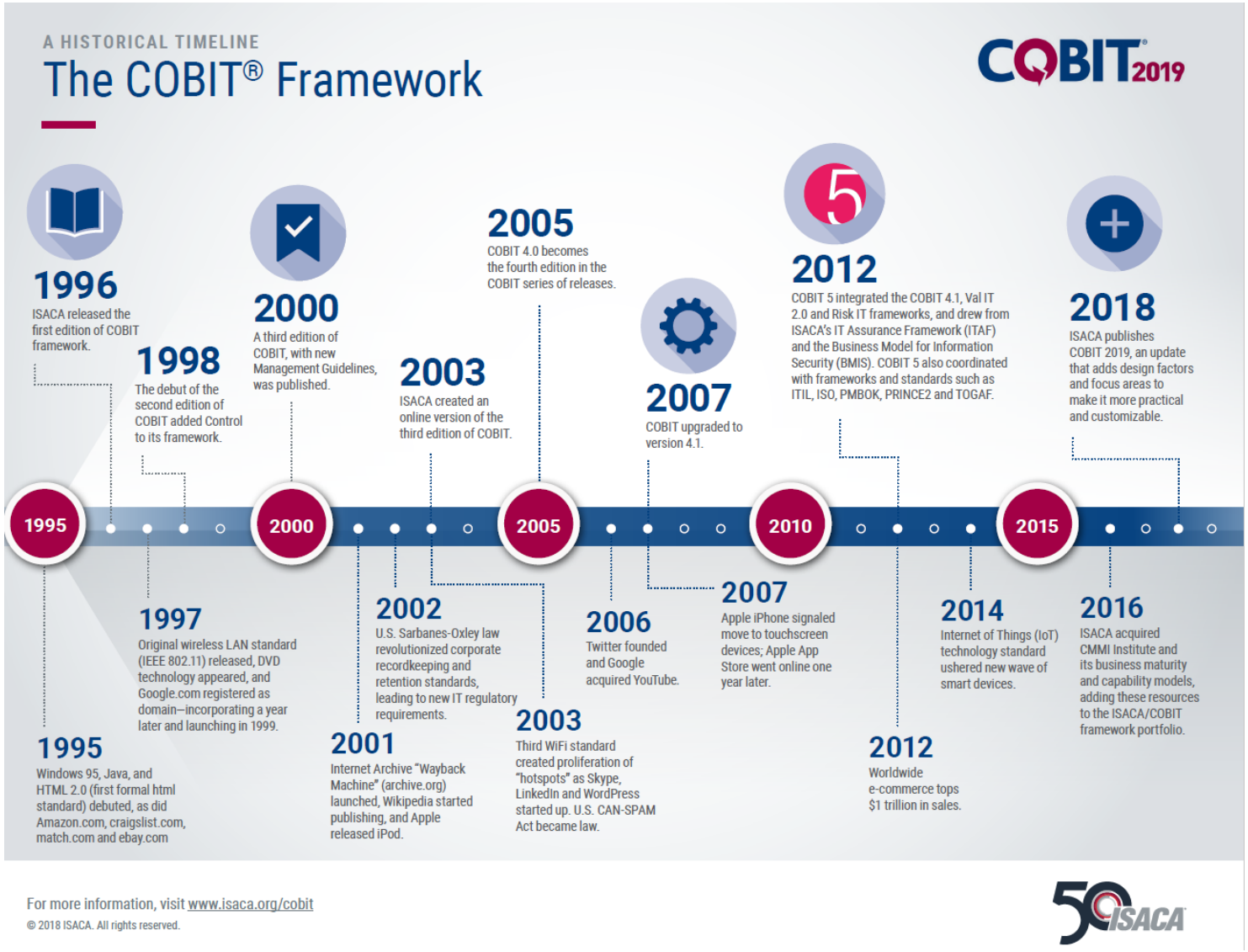
- …definiert die Komponenten für den Aufbau und die Aufrechterhaltung eines Governance-Systems: Prozesse, Organisationsstrukturen, Richtlinien und Verfahren, Informationsfluss, Kultur und Verhaltensweisen, Fähigkeiten und Infrastruktur
- …definiert die Gestaltungsfaktoren, die das Unternehmen beim Aufbau eines optimalen Governance-Systems berücksichtigen sollte

COBIT ✗

- .. ist keine vollständige Beschreibung der gesamten IT-Umgebung eines Unternehmens
- … ist kein Rahmenwerk zur Organisation von Geschäftsprozessen
- … ist kein IT- Rahmenwerk zum Management der gesamten Technologie
- …trifft keine IT-bezogenen Entscheidungen

Quelle: ISACA (Hrsg.) COBIT 2019 Framework Governance and Management Objectives , http://www.isaca.org/

COBIT: Überblick



https://www.isaca.org/resources/infographics/the-cobit-framework-timeline

COBIT: Definition

COBIT …

… ist ein Framework, das Unternehmen beim Erfüllung ihrer Geschäftsstrstegie unterstützt.

… gibt vor, welche Anwendungen und Prozesse innerhalb eines Unternehmens zum Einsatz kommen sollten, um eine effiziente Governance zu gewährleisten.

… hat das Ziel eine gemeinsame Ausrichtung der IT- und Business-Bereiche, innerhalb des Unternehmens zu gewährleisten.

COBIT: Ziele

1. Realisierung von geschäftlichem Nutzen durch eine effiziente und innovative Nutzung der Unternehmens-IT
2. Bereitstellung akkurater Informationen für Geschäftsentscheidungen
3. Erreichen strategischer Ziele mithilfe der IT
4. Identifizierung und Minimieren IT-bezogener Risiken
5. Implementierung von effektivem und verlässlichem Einsatz der Unternehmenstechnologie
6. Erfüllung rechtlicher Auflagen und Verordnungen
7. Einsparung von Kosten und Ressourcen

COBIT 5: Governance-Prinzipien

1. Zufriedenstellung der Stakeholder
   - Mehrwert
2. Abdeckung der gesamten Unternehmens-IT
   - End-to-End-Ansatz
3. Anwendung eines einzigen integrierten Frameworks
   - Konsistenz und Einheitlichkeit
4. Verfolgen eines ganzheitlichen Ansatzes
   - Gemeinsame Prinzipien und Richtlinien
5. Trennung von Governance und Management
   - Führungsebene und Verwaltungsebene

COBIT Core Model: „Governance and Management Objectives“

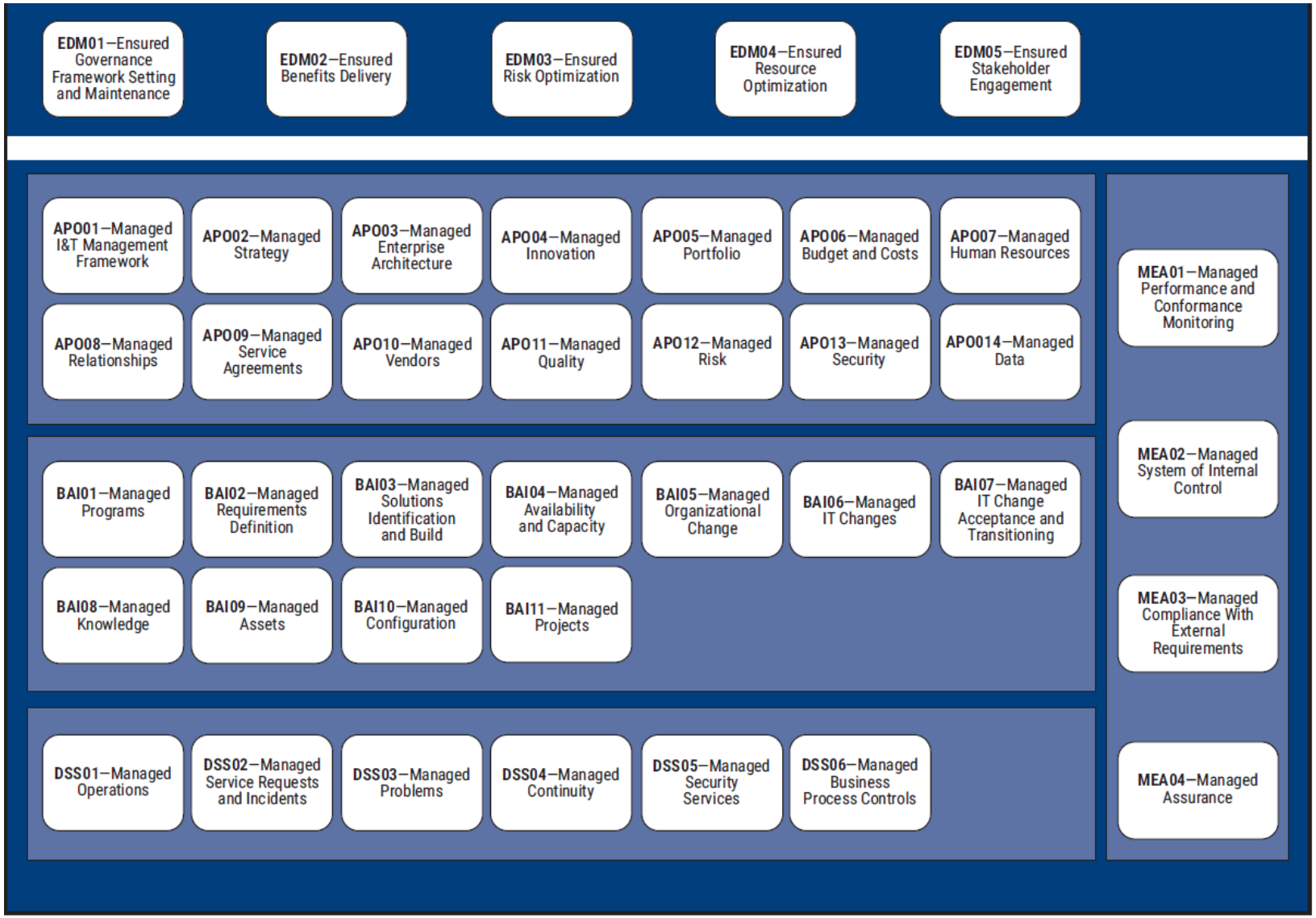
NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Evaluate,
Direct and Monitor

Align, Plan and
Organize

Build, Acquire and
Implement

Deliver, Service and
Support



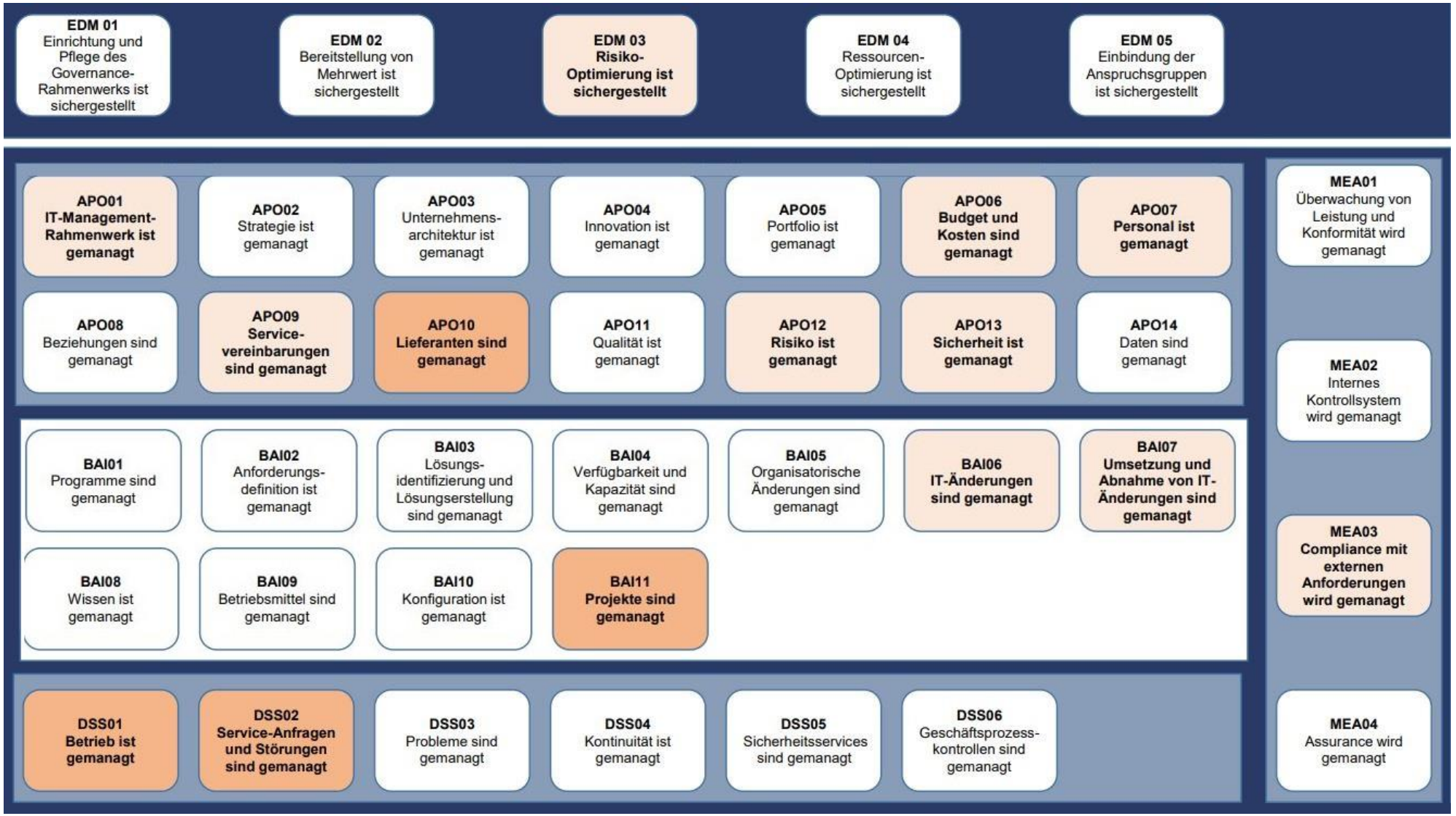
Monitor,
Evaluate and
Assess

Quelle: ISACA (Hrsg.) COBIT 2019 Framework Governance and Management Objectives , http://www.isaca.org/

COBIT for Small and Medium Enterprises (SME)

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Für KMU **wichtige (hell unterlegte)**
oder **sehr wichtige (dunkel unterlegte)**
Governance- und Managementziele
im COBIT 2019-Kernmodell



COBIT Zielhierarchie (Beispiel)

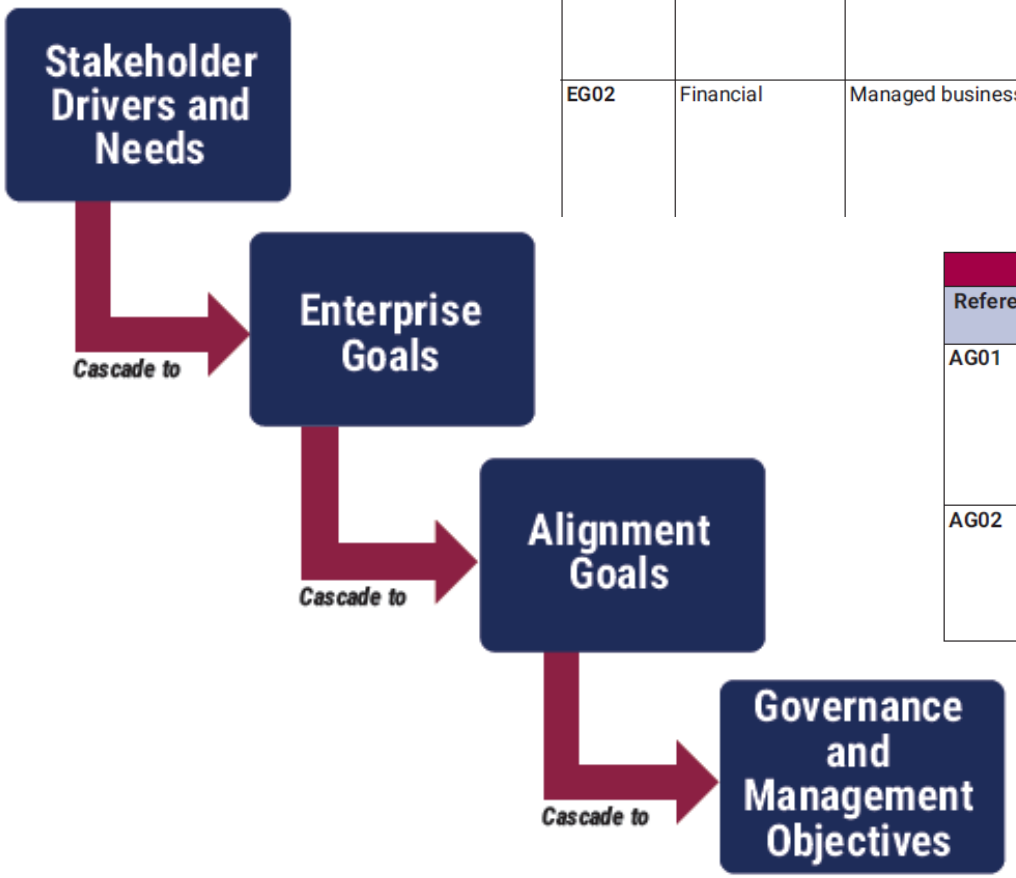


Figure 4.17—Goals Cascade: Enterprise Goals and Metrics

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG01	Financial	Portfolio of competitive products and services	• Percent of products and services that meet or exceed targets in revenues and/or market share • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage • Time-to-market for new products and services
EG02	Financial	Managed business risk	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Appropriate frequency of update of risk profile

Figure 4.18—Goals Cascade: Alignment Goals and Metrics

Reference	IT BSC Dimension	Alignment Goal	Metrics
AG01	Financial	I&T compliance and support for business compliance with external laws and regulations	• Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss • Number of IT-related noncompliance issues reported to the board or causing public comment or embarrassment • Number of noncompliance issues relating to contractual agreements with IT service providers
AG02	Financial	Managed I&T-related risk	• Appropriate frequency of update of risk profile • Percent of enterprise risk assessments including I&T-related risk • Number of significant I&T-related incidents that were not identified in a risk assessment

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose *(cont.)*

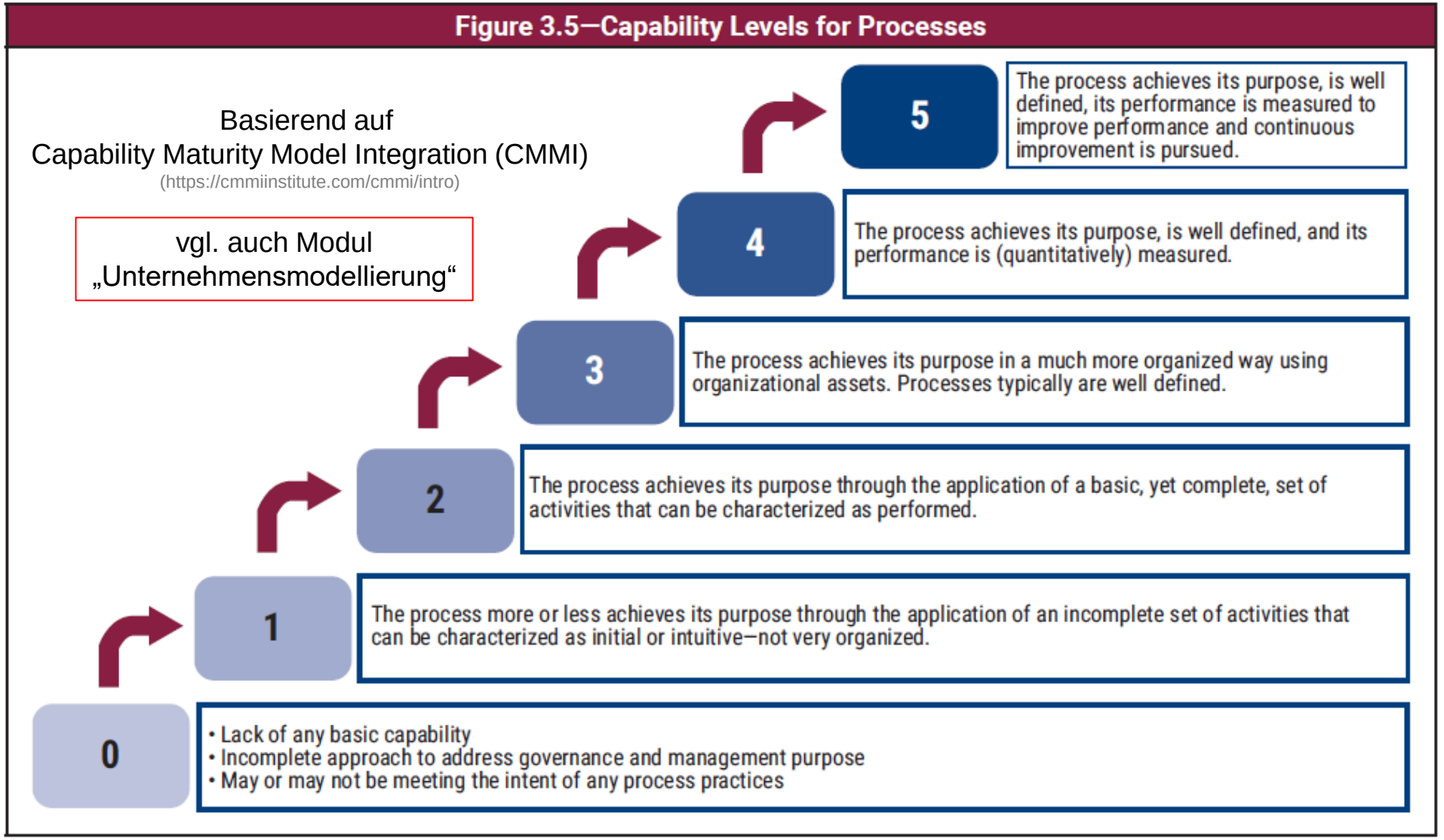
Reference	Name	Purpose
APO12	Managed risk	Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.

Quelle: ISACA (Hrsg.) COBIT 2019 Framework Introduction and Methodology, http://www.isaca.org/

COBIT Framework: Capability Levels

Basierend auf
Capability Maturity Model Integration (CMMI)
(https://cmmiinstitute.com/cmmi/intro)

vgl. auch Modul „Unternehmensmodellierung“



Quelle: ISACA (Hrsg.) COBIT 2019 Framework Governance and Management Objectives , http://www.isaca.org/

COBIT Framework: Capability Levels (Beispiel)

„Management Practices“

„Capability Levels“

„Activities“

Management Practice	Example Metrics	
APO12.02 Analyze risk. Develop a substantiated view on actual I&T risk, in support of risk decisions.	a. Number of identified I&T risk scenarios b. Time since last update of I&T risk scenarios	
Activities		**Capability Level**
1. Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.		3
2. Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.		
3. Estimate the frequency (or likelihood) and magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.		
4. Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.		
5. Propose risk responses for risk exceeding risk appetite and tolerance levels.		
6. Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.		
7. Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.		4
8. Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.		5

Quelle: ISACA (Hrsg.) COBIT 2019 Framework Governance and Management Objectives , http://www.isaca.org/

COBIT: Rollen und Verantwortlichkeiten

Beispiel / Ausschnitt

Rollen in der Organisation

„Management Practices“

Verantwortlichkeiten (RACI -Modell)

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Analyze risk.	A	R			R		R										
APO12.03 Maintain a risk profile.	A	R			R		R										
APO12.04 Articulate risk.	A	R			R		R										
APO12.05 Define a risk management action portfolio.	A	R			R		R										
APO12.06 Respond to risk.	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

Quelle: ISACA (Hrsg.) COBIT 2019 Framework Governance and Management Objectives , http://www.isaca.org/

RACI-Matrix: Erläuterung

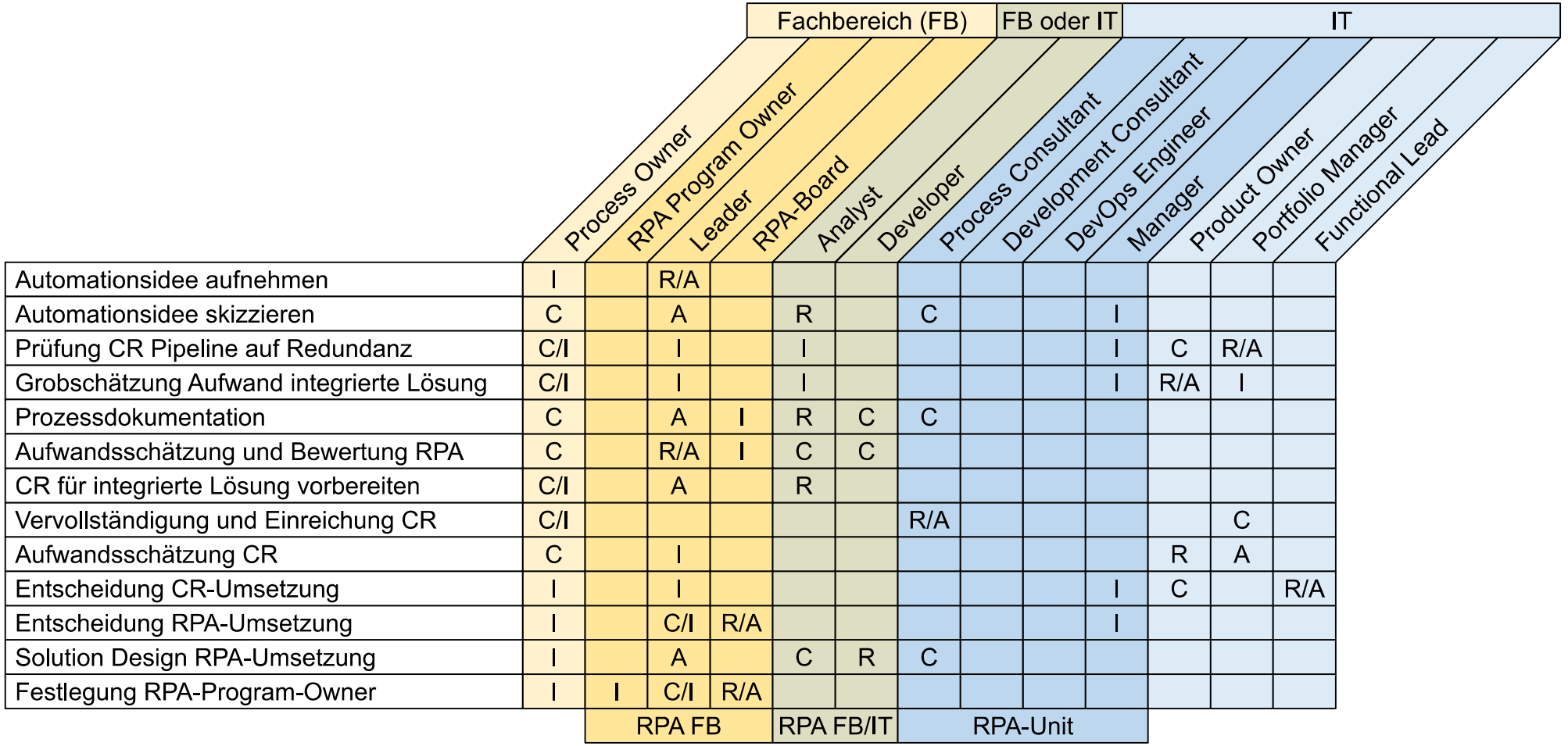
Codierung	Erklärung
Responsible	Wer ist für die Ausführung der Aufgabe verantwortlich? (Durchführungsverantwortung)
Accountable	Wer ist für das Ergebnis der Aufgabe verantwortlich bzw. wer gibt es frei? (Rechenschaftspflicht, Kostenverantwortung)
Consulted	Wer ist Experte und kann zur Ausführung der Aufgabe befragt werden?
Informed	Wer wird über den Arbeitsfortschritt der Aufgabe informiert?

Erweiterungen / Varianten z.B.:

- RA**S**CI - Zusätzliche Rolle "Support": Wer trägt zur Erfüllung der Aufgabe bei?
- RACI**Q** - Zusätzliche Rolle "Quality Review": Wer prüft die Einhaltung der Qualitätsanforderungen?

https://www.projektmagazin.de/methoden/verantwortlichkeitsmatrix-raci-matrix

RACI-Matrix: Beispiel zur Anwendung



	Fachbereich (FB)				FB oder IT		IT						
	Process Owner	RPA Program Owner	Leader	RPA-Board	Analyst	Developer	Process Consultant	Development Consultant	DevOps Engineer	Manager	Product Owner	Portfolio Manager	Functional Lead
Automationsidee aufnehmen	I		R/A										
Automationsidee skizzieren	C		A		R		C			I			
Prüfung CR Pipeline auf Redundanz	C/I		I		I					I	C	R/A	
Grobschätzung Aufwand integrierte Lösung	C/I		I		I					I	R/A	I	
Prozessdokumentation	C		A	I	R	C	C						
Aufwandsschätzung und Bewertung RPA	C		R/A	I	C	C							
CR für integrierte Lösung vorbereiten	C/I		A		R								
Vervollständigung und Einreichung CR	C/I						R/A					C	
Aufwandsschätzung CR	C		I								R	A	
Entscheidung CR-Umsetzung	I		I							I	C		R/A
Entscheidung RPA-Umsetzung	I		C/I	R/A						I			
Solution Design RPA-Umsetzung	I		A		C	R	C						
Festlegung RPA-Program-Owner	I	I	C/I	R/A									
		RPA FB			RPA FB/IT		RPA-Unit						

Petersen, J.; Schröder, H.: Entwicklung einer Robotic Process Automation (RPA)-Governance, HMD Praxis der Wirtschaftsinformatik, 57 (2020)
https://link.springer.com/article/10.1365/s40702-020-00659-y

KI-Governance

- KI-Governance:
  - **Rahmenbedingungen, Richtlinien und Praktiken**, die sicherstellen, dass KI **verantwortungsvoll, ethisch und im Einklang mit menschlichen Werten** entwickelt und eingesetzt wird
  - Steuerung der Entwicklung und Anwendung von KI-Systemen, dass sie den Interessen der Gesellschaft dienen, Risiken minimieren und positive Auswirkungen maximieren
- KI-Governance umfasst u. a. Aspekte wie

  ⇒ **Transparenz, Verantwortlichkeit, Fairness, Datenschutz, Sicherheit und menschliche Werte**
- Da KI-Technologien den beruflichen und privaten Alltag immer stärker beeinflussen, ist eine wirksame Governance unerlässlich!
- KI-Governance dient dazu, Missbrauch zu verhindern, Vertrauen in KI-Systeme aufzubauen und sicherzustellen, dass diese Technologien zum „Wohl der Gesellschaft“ beitragen
- Ohne angemessene Governance könnten KI-Systeme unbeabsichtigten Schaden erzeugen, ethische Grundsätze verletzen oder zu Ungleichheiten beitragen …

KI-Governance

Warum sind die **Grundprinzipien**

- Transparenz,
- Verantwortlichkeit,
- Fairness,
- Datenschutz,
- Sicherheit und
- menschliche Werte

wichtig für eine **KI-Governance**?

KI-Governance – Grundprinzipien (1)

1. Transparenz

- Transparenz ist entscheidend, um Vertrauen in KI-Systeme aufzubauen
- Dies bedeutet, dass die Funktionsweise und Entscheidungsfindung der KI für Nutzer und Betroffene nachvollziehbar sein sollte
- Transparenz beinhaltet auch die Offenlegung, wie Daten gesammelt, analysiert und verwendet werden

2. Verantwortlichkeit

- Es muss klar definiert sein, wer für die Handlungen und Entscheidungen einer KI verantwortlich ist
- Dies umfasst sowohl die rechtliche als auch die ethische Verantwortung
- Verantwortlichkeit stellt sicher, dass bei Fehlern oder Missbrauch von KI-Systemen jemand zur Rechenschaft gezogen werden kann

3. Fairness

- KI-Systeme sollten frei von Vorurteilen sein und alle Nutzer gleich behandeln
- Dies erfordert sorgfältige Prüfung und Anpassung der Algorithmen, um Diskriminierung und Verzerrungen zu vermeiden
- Fairness in der KI bedeutet auch, dass die Vorteile der KI-Technologie breit und gerecht in der Gesellschaft verteilt werden

KI-Governance – Grundprinzipien (2)

4. Datenschutz

- Der Schutz persönlicher Daten ist ein zentrales Element der KI Governance
- KI-Systeme müssen so gestaltet sein, dass sie die Privatsphäre der Nutzer respektieren und die Datensicherheit gewährleisten
- Dies beinhaltet auch die Einhaltung von Datenschutzgesetzen und -richtlinien

5. Sicherheit

- KI-Systeme müssen sicher und robust gegen Manipulationen und Fehlfunktionen sein
- Dies schließt die Entwicklung von Mechanismen ein, um Missbrauch zu verhindern und die Integrität der KI-Systeme zu gewährleisten

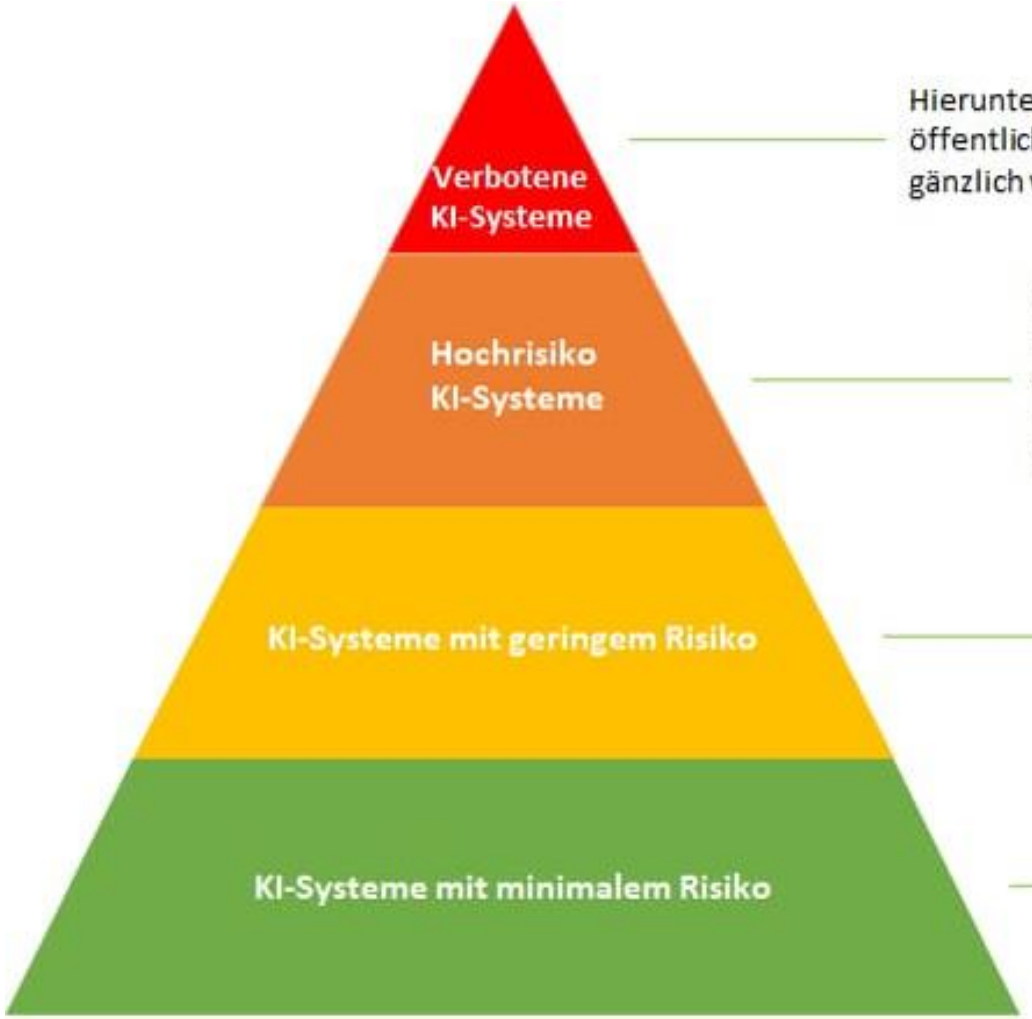
6. Menschliche Werte

- Die Entwicklung und Anwendung von KI sollte im Einklang mit grundlegenden menschlichen Werten und ethischen Grundsätzen stehen
- Des beinhaltet Respekt für die menschliche Autonomie, Gerechtigkeit, Wohlergehen und die Förderung des gesellschaftlichen Gutes

KI-Governance – Fazit

- Die Grundprinzipien sind entscheidend, um das Vertrauen der Öffentlichkeit in KI-Technologien zu stärken und sicherzustellen, dass ihre Entwicklung und Anwendung im Interesse der Menschen erfolgt
- Die Governance der KI ist dabei nicht nur eine technische, sondern auch eine soziale und ethische Frage
- Sie spielt eine entscheidende Rolle, wenn es darum geht, das Potenzial der KI voll auszuschöpfen und gleichzeitig ihre Risiken zu minimieren
- Eine wirksame KI-Governance fördert Innovationen, die im Einklang mit menschlichen Werten und gesellschaftlichen Zielen stehen
- Sie ist der Schlüssel dafür, dass KI-Technologien zum Nutzen aller eingesetzt werden und eine positive Zukunft gestalten

EU-Gesetz über künstliche Intelligenz



Hierunter fallen etwa KI-Systeme zum Social Scoring, zur biometrischen Identifizierung in Echtzeit im öffentlichen Raum oder zur Verhaltensmanipulation. Diese KI-Systeme sind nach Art. 5 KI-Verordnung gänzlich **verboten**.

In diese Kategorie fallen KI-Systeme, die in den Produktsicherheitsvorschriften der EU unterfallenden Produkten eingesetzt werden oder ein solches Produkt sind oder in Anlage III aufgeführt werden (etwa Verwaltung und Betrieb kritischer Infrastrukturen oder im Bereich Beschäftigung und Personalmanagement. Diese KI-Systeme unterliegen nach Art. 6 bis 51 KI-Verordnung einer **umfassenden Regulierung** und weitreichenden Verpflichtungen.

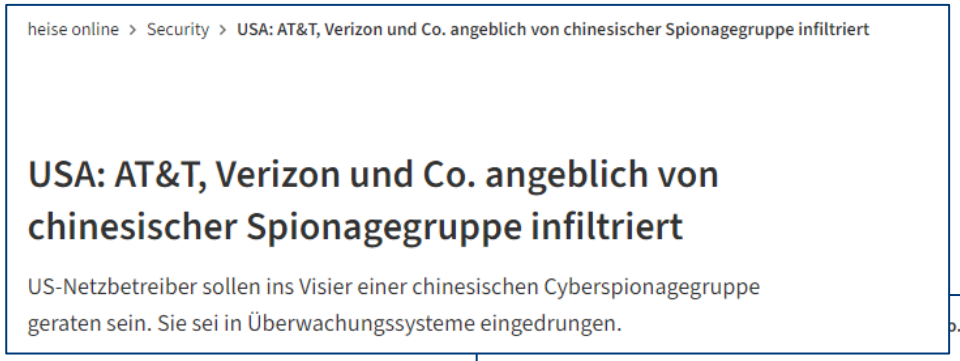
Hierunter fallen etwa solche Systeme, mit denen Menschen direkt interagieren können (etwa ein Chatbot). Diese KI-Systeme unterliegen den **Transparenzpflichten** nach Art. 52 KI-Verordnung.

Beispiele hierfür sind etwa KI in Computerspielen oder KI-gestützte Spamfilter. Diese KI-Systeme unterfallen dem Anwendungsbereich der KI-Verordnung nicht und unterliegen insofern **keinen Beschränkungen**.

Inhalt

- Überblick
- IT-Strategie
- IT-Governance, Risikomanagement und Compliance
  - IT-Governance
  - IT-Risikomanagement
  - IT-Compliance
- IT-Organisation
- IT-Outsourcing
- IT-Servicemanagement

IT-Risiken


heise online > Security > USA: AT&T, Verizon und Co. angeblich von chinesischer Spionagegruppe infiltriert

USA: AT&T, Verizon und Co. angeblich von chinesischer Spionagegruppe infiltriert

US-Netzbetreiber sollen ins Visier einer chinesischen Cyberspionagegruppe geraten sein. Sie sei in Überwachungssysteme eingedrungen.


heise online > Security > Attacke auf Online-Apotheke DocMorris: 20.000 Kundenkonten betroffen

Attacke auf Online-Apotheke DocMorris: 20.000 Kundenkonten betroffen

DocMorris zufolge kompromittierten Hacker 20.000 Konten aufgrund "mehrfach verwendeter Passwörter". Daraufhin wurden Konten vorsorglich gesperrt.


o.: Störung legte Apps lahm

Microsoft Outlook, Teams & Co.: Störung legte Apps lahm

Microsofts Cloud-Service liefen am Morgen des 25. Januar nicht rund. Konferenzen über Teams starteten praktisch nicht, andere Microsoft-365-Apps luden langsam.


heise online > Security > CrowdStrike-Fiasko: Neue Details zum fatalen Update, BSI warnt vor Angriffen

CrowdStrike-Fiasko: Neue Details zum fatalen Update, BSI warnt vor Angriffen

Die Wurzel allen Übels hat einen Namen: Das Channel File 291 hat weltweit für massive IT-Ausfälle gesorgt. Das BSI warnt unterdessen vor CrowdStrike-Phishing.


heise online > Digitalisierung > Digital Health > 38C3: Große Sicherheitsmängel in elektronischer Patientenakte 3.0 aufgedeckt

38C3: Große Sicherheitsmängel in elektronischer Patientenakte 3.0 aufgedeckt

Gravierende Sicherheitslücken müssten bis zum Start der ePA 3.0 noch geschlossen werden. Das demonstrieren Martin Tschirsich und Bianca Kastl auf dem 38C3.


heise online > Luftfahrt > Flugchaos in den USA: "Unabsichtlich" gelöschte Dateien als Ursache

Flugchaos in den USA: "Unabsichtlich" gelöschte Dateien als Ursache

Bei Arbeiten am System für das Backup einer wichtigen Datenbank seien versehentlich Dateien gelöscht worden, teilte die FAA jetzt mit. Man habe nachgebessert.

⇒ Effektives IT-Risikomanagement !!!

IT-Risikomanagement

Das Erkennen und Beherrschen der IT Risiken ist eine strategische Aufgabe

- Die Unternehmen sind bei der Durchführung Ihrer Geschäftsprozesse von der Verfügbarkeit und der Qualität der IT-Systeme abhängig
- Der Ausfall der IT kann dramatische Konsequenzen haben

Begriff „Risiko“

- Auf die Zukunft gerichtete Betrachtung
- Unsicherheit bezüglich künftiger Entwicklung
- Möglichkeit eines Schadens oder einer negativen Entwicklung

Quelle: Tiemeyer, E.: Handbuch IT-Management

Definitionen nach BSI

*„Eine **Bedrohung** (threat) ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann“*

+

„Eine **Schwachstelle** (vulnerability) ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution“

=

„Eine **Gefährdung** (applied threat) ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt“

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Glossar
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Definitionen nach BSI

„Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit.“

„Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.“

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Glossar
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Risiko = Wahrscheinlichkeit * Schaden

Motivation für ein IT-Risikomanagement

intern motiviert

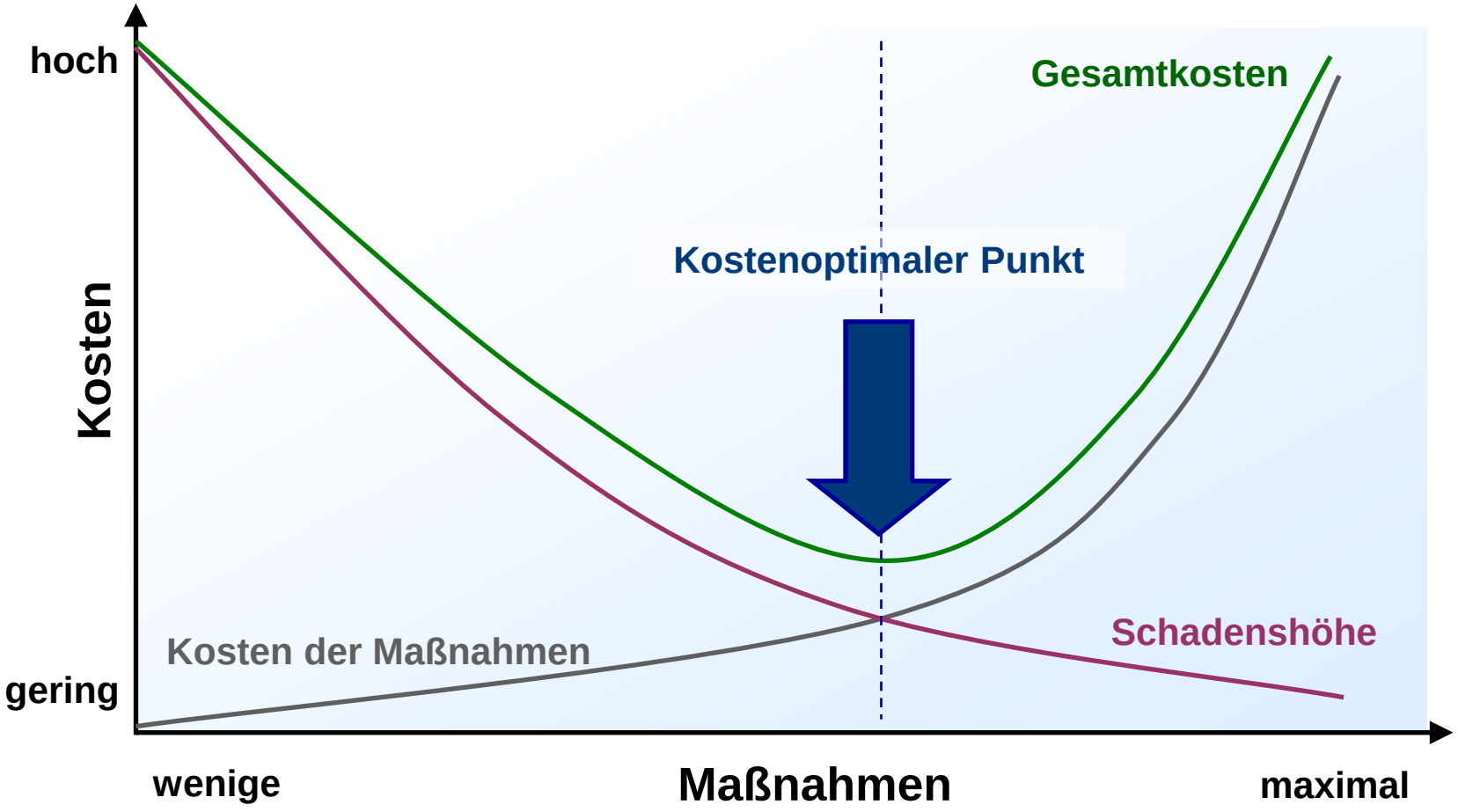
- betriebswirtschaftliche Notwendigkeit
- Risikoaffinität/-kultur des Managements

extern motiviert

- KonTraG
- Sarbanes-Oxley Act
- 8. EU Richtlinie, BilMoG
- Bundesdatenschutzgesetz
- IT-Sicherheitsgesetz
- EU DSGVO…

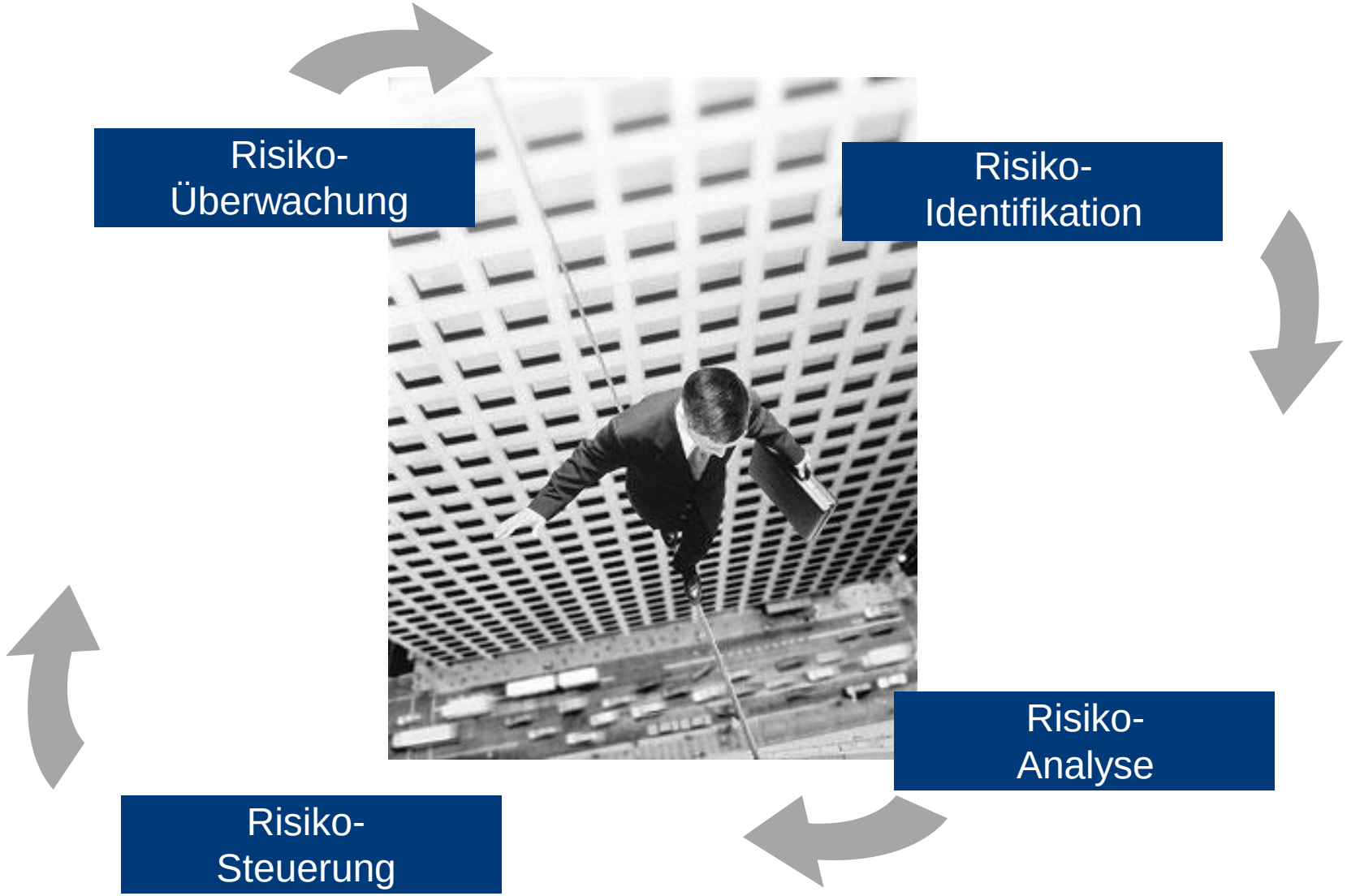
Forderung nach einem systematischen IT-Risikomanagement

IT-Risikomanagement: wirtschaftliche Betrachtung



Risikomanagement: Prozess

Risikomanagement: Prozess

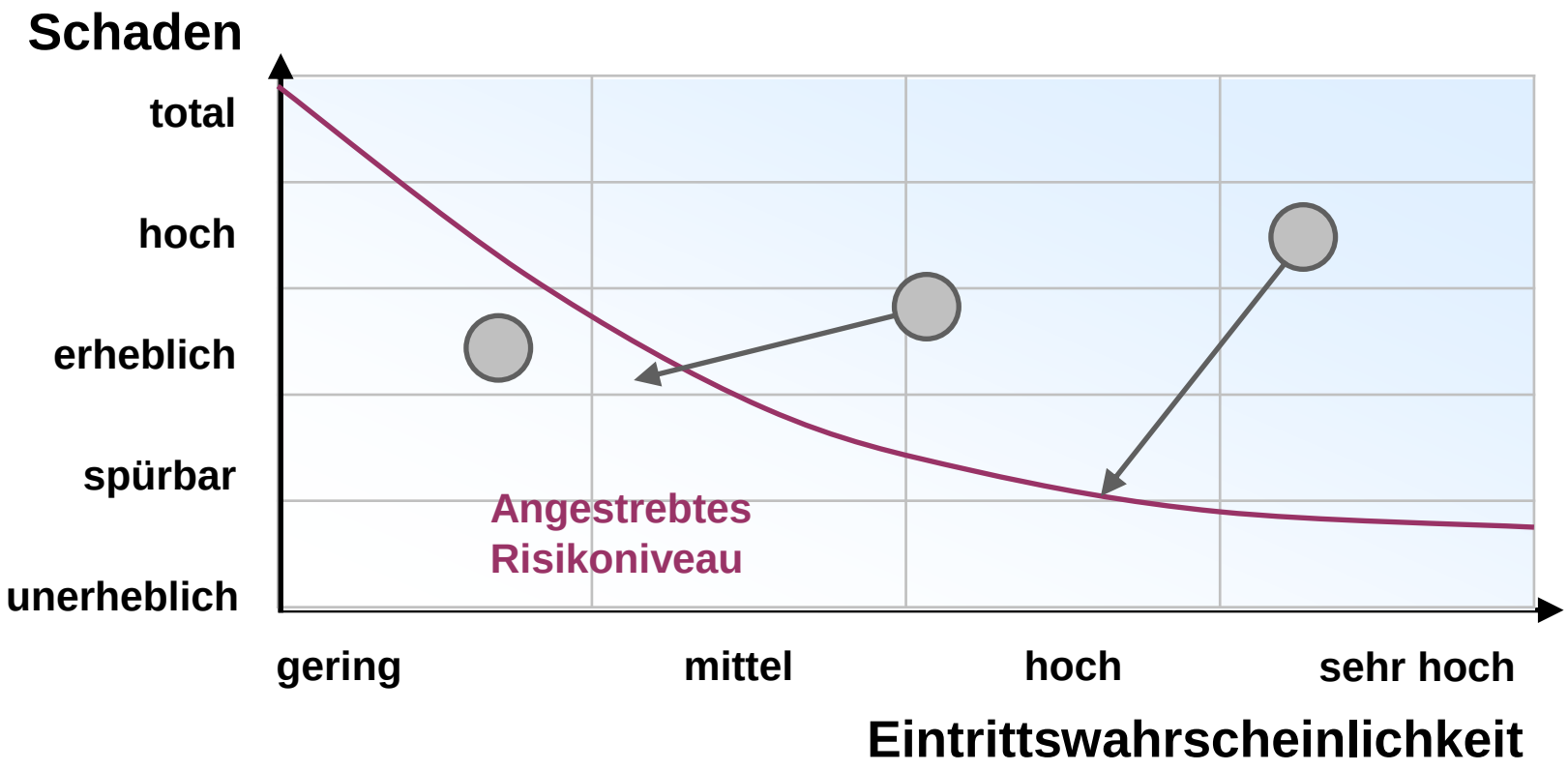


Risikoidentifikation

- Erkennen existierender und künftige Risiken
- Techniken:
  - Checklisten, Risikokataloge
  - Analyse vergangener Schadensfälle
  - Szenarioanalysen
  - Expertenbefragungen
  - Befragung von Anwendern, IT-Mitarbeitern

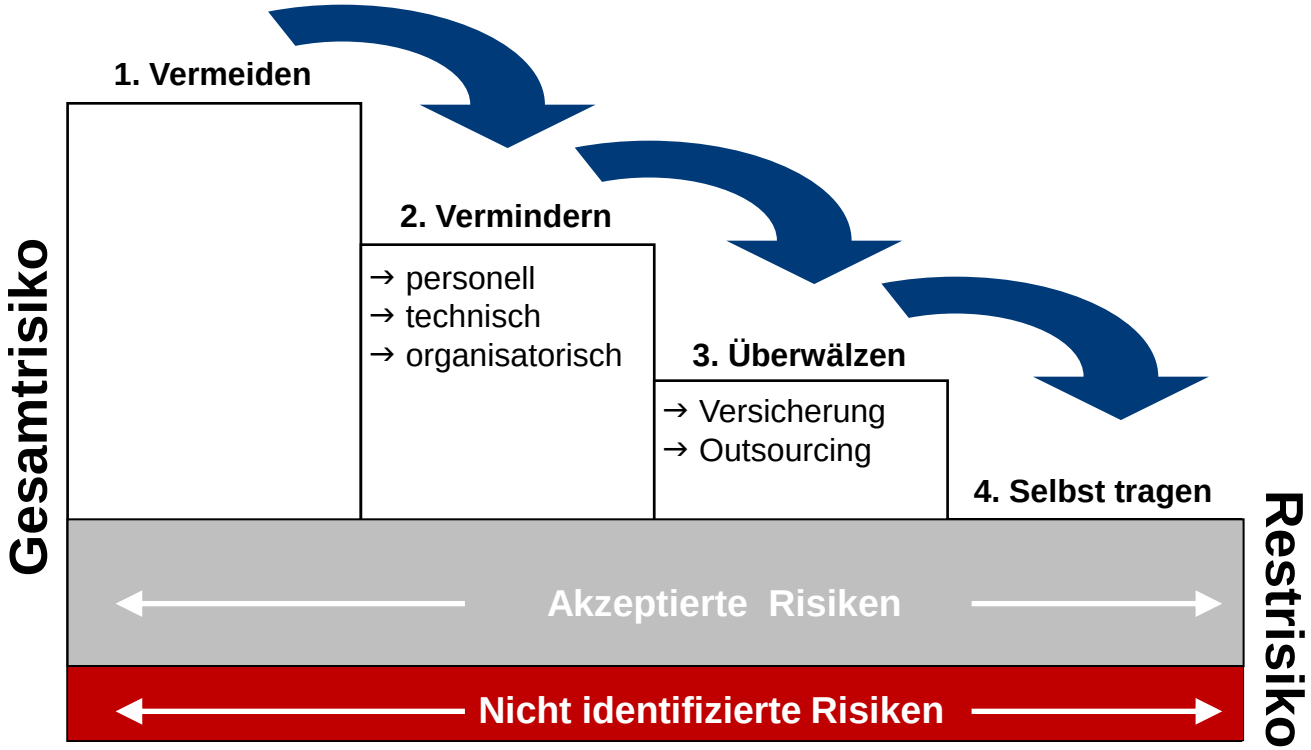
Risikoanalyse

- Abschätzung von Eintrittswahrscheinlichkeit und Schadenshöhe
- quantitative / qualitative Bewertung



Risikosteuerung

- Abgleich der analysierten Risiken mit Zielen / Risikostrategie
- Beeinflussung der Ursachen (Eintrittswahrscheinlichkeit) und der Auswirkungen (Schadenshöhe)



Risikosteuerung: Instrumente

Instrument	Maßnahmen	Anwendungsbereiche
Risiko-Vermeidung	Risikoreduktion auf ein Restrisiko von Null, bspw. Abschaffung eines Systems, Abbruch eines Projekts	Vorwiegend bei Risikoeinstufung „sehr hoch“ oder „hoch“
Risiko-Verminderung	Reduktion der Eintrittswahrscheinlichkeit und Verringerung der Schadenswirkungen, aktive Beeinflussung der Ursachen	Vorwiegend bei Risikoeinstufung „hoch“ oder „mittel“
Risiko-Überwälzung	Übertragung möglicher Störungen vor ihrem Eintritt auf andere Wirtschaftssubjekte, bspw. Outsourcing oder Versicherung	Anwendung bei allen Risikoeinstufungen möglich.
Risiko-Selbsttragung	Bewusste Akzeptanz des (Rest-)Risikos, im Rahmen unternehmerischen Handelns nicht eliminierbar, ggf. Bildung von finanziellen oder materiellen Reserven	Management des akzeptierten Restrisikoniveaus („niedrig“, „vernachlässigbar“)
Risiko-Streuung	Einsatz aller Instrumente im Rahmen eines Instrumenten-Mixes	Unterstützendes Instrument beim Einsatz aller anderen Risk Management Instrumente

Risikoüberwachung

- Kontrolle des Erfolges der Steuerungsmaßnahmen
- Überwachen der Restrisiken
- Erkennen von Änderungen der Risikolage
- Erkennen bisher nicht identifizierter Risiken
- Reporting

Zentrale Rollen im IT-Risikomanagement: Vorschlag

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

„Chief Information Risk Officer“

- Definiert methodische Vorgaben
- Legt Policies fest

„IT Risk Owner“

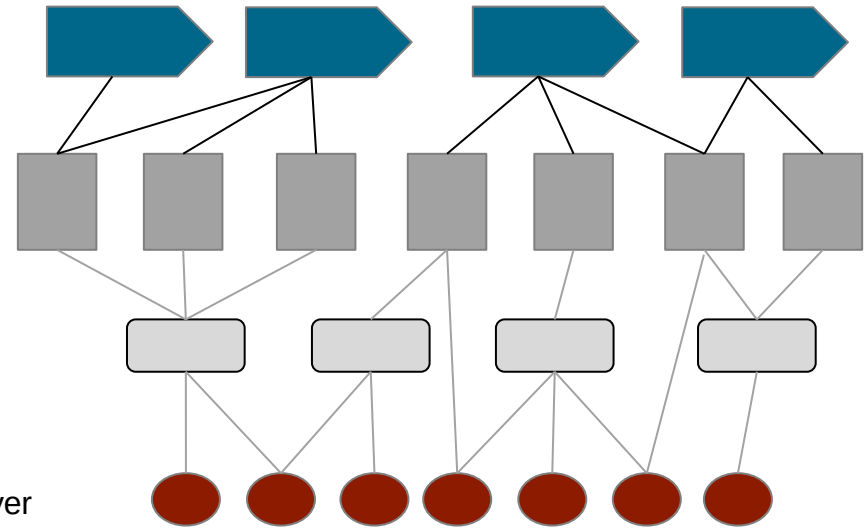
- Ist von Schäden unmittelbar betroffen
- Stellt Anforderungen an das IT-Risikomanagement

„IT Risk Manager“

- Bewertet die IT Risiken
- Definiert Maßnahmen

„System-verantwortlicher“

- Setzt Maßnahmen auf operativer Ebene um
- Identifiziert Schwachstellen



Quelle: e-ThinkTank / Arbeitskreis IT mit Zukunft

tagesschau

Sendung verpasst?

Startseite ▸ Ausland ▸ Banken, Flughäfen, Kliniken: Weltweit Störungen bei Computersystemen

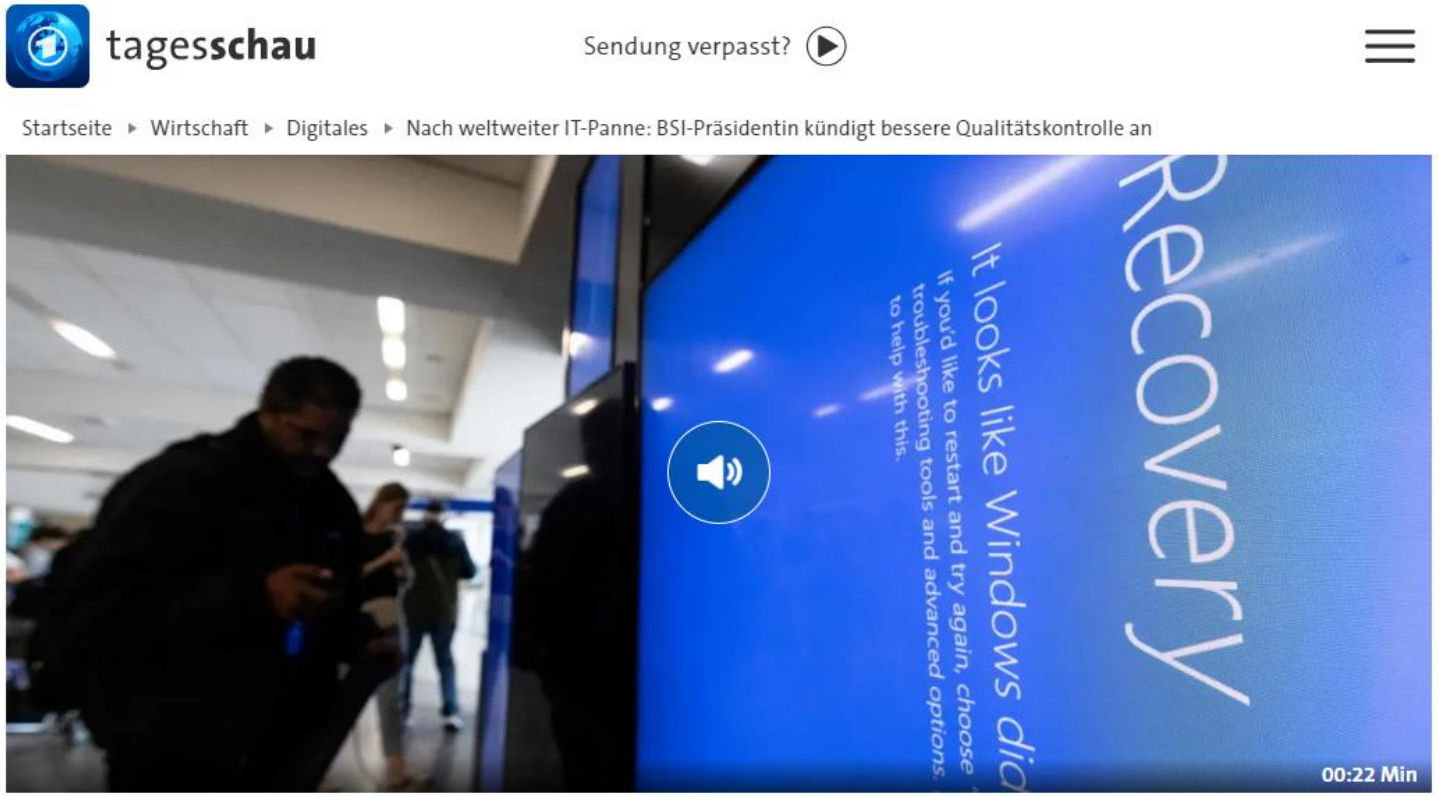
Banken und Flughäfen betroffen

Weltweit Störungen bei Computersystemen

Stand: 19.07.2024 12:52 Uhr

Fluggesellschaften, Banken oder Medienhäuser: Aus mehreren Staaten werden massive Probleme bei Computersystemen gemeldet. Auch Deutschland ist massiv betroffen. Die Störung könnte mit einem fehlerhaften Software-Update zu tun haben.

www.tagesschau.de/ausland/it-panne-computer-global-100.html



Nach weltweiter IT-Panne

BSI-Präsidentin kündigt bessere Qualitätskontrolle an

Stand: 20.07.2024 11:13 Uhr

Weltweit dauert die Wiederherstellung der IT-Systeme nach der Panne an. Am Flughafen BER läuft der Betrieb wieder weitgehend normal. BSI-Chefin Plattner kündigt Konsequenzen aus dem IT-Ausfall an - und dämpft gleichzeitig Erwartungen.

www.tagesschau.de/wirtschaft/digitales/crowdstrike-it-ausfall-100.htm

Rahmenwerke/Standards: ISO/IEC 27000-Reihe

Normenreihe zur Informationssicherheit, u.a.:

http://www.iso.org

http://www.bsigroup.com

- ISO/IEC 27001
  - spezifiziert die Anforderungen für die Erstellung, die Einführung, den Betrieb, die Überwachung, die Wartung und die Verbesserung eines Information Security Management Systems (ISMS).
  - entwickelt aus dem British Standard 7799
  - Spezifiziert die zu implementierenden Sicherheitsmaßnahmen nach Erfordernis der jeweiligen Organisation
  - stellt keine konkreten Anforderungen bzgl. Ausführung der Maßnahmen
  - definiert Zertifizierungsanforderungen

- ISO/IEC 27002 (ehemals ISO 17799)
  - Code of practice for information security management
  - Sammlung von Empfehlungen für IT-Sicherheitsverfahren und -methoden, die sich in der Praxis bewährt haben
  - Enthält „Kontrollziele“ und kann als Leitfaden für die Implementierung eines Information Security Management Systems dienen

Rahmenwerke / Standards: IT-Grundschutz

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

> *„Der IT-Grundschutz […] ist Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen, die sich mit der Absicherung ihrer Daten, Systeme und Informationen befassen wollen. Zentral ist dabei ein ganzheitlicher Ansatz zur Informationssicherheit: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. […]*

Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

- Entwickelt und publiziert vom Bundesamt für Sicherheit in der Informationstechnik
- Enthält konkrete Vorgaben für IT-Strukturanalyse, Schutzbedarfsfeststellung, Sicherheitschecks und Umsetzung
- Hoher Detaillierungs- / Operationalisierungsgrad (nicht nur „was“, sondern auch „wie“)
- Beschreibt, wie ein ISMS in der Praxis aufgebaut und betrieben werden kann
  (Aufgaben und Rollen, Maßnahmenauswahl)
- Enthält speziell für kleinere Institutionen einen „Weg in die Basis-Absicherung“
- Ist eine **Konkretisierung** der Erfüllung allgemein gehaltenen Anforderungen aus den **ISO-Standards**
  (Basis für ISO 27001 Zertifizierung – auch international angesehen)

Rahmenwerke / Standards: IT-Grundschutz

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-kompendium

- Zertifizierungsgrundlage nach ISO 27001 auf Basis von IT-Grundschutz
- Einführung in die IT-Grundschutz-Methodik
- > 90 (modernisierte) Prozess- und System-Bausteine

BSI-Standards
200-1, 200-2, 200-3
100-4

- 200-1: Managementsysteme für Informationssicherheit
- 200-2: IT-Grundschutz-Methodik
- 200-3: Risikomanagement
- 100-4: Notfallmanagement
- Erweitert um die Themen Virtualisierung, Absicherung von IoT, Clouds sowie ICS

Weg in die Basisabsicherung (WiBA)

- Beschreibung grundlegender Schritte zur Umsetzung erster Sicherheitsmaßnahmen
- Speziell für kleinere Institutionen, die sich erstmals mit Thema IT-Sicherheit auseinandersetzen

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Zentrale Rollen im IT-Grundschutz

Rollen

In den Anforderungen werden neben der eigentlichen Empfehlung beispielhaft Zuständige für die Initiierung bzw. für die Erfüllung dieser Anforderung genannt. Da die Bezeichnungen der hier als Zuständige genannten Personen oder Rollen nicht in allen Organisationen einheitlich sind, wird für eine leichtere Zuordnung in diesem Kapitel eine kurze Beschreibung der wesentlichen Rollen dargestellt.

Name	Beschreibung
Anforderungsmanager (Compliance Manager)	Der Anforderungsmanager (Compliance Manager) ist verantwortlich dafür, die für die Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren und deren Einhaltung zu prüfen.
Auditteam	Das Auditteam besteht aus Auditoren und Fachexperten, die den Auditteamleiter insbesondere fachlich während eines Audits unterstützen.
Bauleiter	Ein Bauleiter ist für die Umsetzung von Baumaßnahmen zuständig.
Benutzer	Ein Benutzer ist ein Mitarbeiter einer Institution, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt. IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben verwendet.
Bereichssicherheitsbeauftragter	Der Bereichssicherheitsbeauftragte ist für alle Sicherheitsbelange der Geschäftsprozesse, Anwendungen und IT-Systeme in seinem Bereich (z. B. Abteilung oder Außenstelle) zuständig. Je nach Größe des zu betreuenden Bereichs kann die Aufgabe des Bereichssicherheitsbeauftragten von einer Person übernommen werden, die bereits mit ähnlichen Aufgaben betraut ist.
Beschaffungsstelle	Die Beschaffungsstelle initiiert und überwacht Beschaffungen. Öffentliche Einrichtungen wickeln ihre Beschaffungen nach vorgeschriebenen Verfahren ab. Die Rolle Beschaffungsstelle schließt den zuständigen Leiter der Organisationseinheit mit ein.
Brandschutzbeauftragter	Ein Brandschutzbeauftragter ist Ansprechpartner und Verantwortlicher in allen Fragen des Brandschutzes. Er ist u. a. zuständig für die Erstellung von Brandrisikoanalysen, Aus- und Fortbildung der Beschäftigten, teilweise auch für Wartung und Instandhaltung der Brandschutzeinrichtungen.
Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung bestellte Person, die auf den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen bzw. in der Behörde hinwirkt.
Entwickler	Mit Entwickler wird im Kontext des IT-Grundschutzes eine Person bezeichnet, die bei Planung, Entwicklung, Test oder Pflege von Software, Hardware oder ganzen Systemen mitarbeitet. Im IT-Grundschutz werden unter der Rolle Entwickler verschiedene weitere Rollen zusammengefasst, wie z. B. Software-Architekt, Software-Designer, Software-Entwickler, Programmierer und Tester. Die Rolle Entwickler schließt den zuständigen Leiter der Organisationseinheit mit ein.

…ca 30 wesentliche Rollen, die in Informationssicherheit nach BSI Grundschutz involviert sind

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Zentrale Rollen im IT-Grundschutz

Rollen

In den Anforderungen werden neben der eigentlichen Empfehlung beispielhaft Zuständige für die Initiierung bzw. für die Erfüllung dieser Anforderung genannt. Da die Bezeichnungen der hier als Zuständige genannten Personen oder Rollen nicht in allen Organisationen einheitlich sind, wird für eine leichtere Zuordnung in diesem Kapitel eine kurze Beschreibung der wesentlichen Rollen dargestellt.

Name	Beschreibung
Anforderungsmanager (Compliance Manager)	Der Anforderungsmanager (Compliance Manager) ist verantwortlich dafür, die für die Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren und deren Einhaltung zu prüfen.
Auditteam	Das Auditteam besteht aus Auditoren und Fachexperten, die den Auditteam-
	schäftsprozesse, Anwendungen und IT-Systeme in seinem Bereich (z. B. Abteilung oder Außenstelle) zuständig. Je nach Größe des zu betreuenden Bereichs kann die Aufgabe des Bereichssicherheitsbeauftragten von einer Person übernommen werden, die bereits mit ähnlichen Aufgaben betraut ist.
Beschaffungsstelle	Die Beschaffungsstelle initiiert und überwacht Beschaffungen. Öffentliche Einrichtungen wickeln ihre Beschaffungen nach vorgeschriebenen Verfahren ab. Die Rolle Beschaffungsstelle schließt den zuständigen Leiter der Organisationseinheit mit ein.
Brandschutzbeauftragter	Ein Brandschutzbeauftragter ist Ansprechpartner und Verantwortlicher in allen Fragen des Brandschutzes. Er ist u. a. zuständig für die Erstellung von Brandrisikoanalysen, Aus- und Fortbildung der Beschäftigten, teilweise auch für Wartung und Instandhaltung der Brandschutzeinrichtungen.
Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung bestellte Person, die auf den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen bzw. in der Behörde hinwirkt.
Entwickler	Mit Entwickler wird im Kontext des IT-Grundschutzes eine Person bezeichnet, die bei Planung, Entwicklung, Test oder Pflege von Software, Hardware oder ganzen Systemen mitarbeitet. Im IT-Grundschutz werden unter der Rolle Entwickler verschiedene weitere Rollen zusammengefasst, wie z. B. Software-Architekt, Software-Designer, Software-Entwickler, Programmierer und Tester. Die Rolle Entwickler schließt den zuständigen Leiter der Organisationseinheit mit ein.

Compliance-Beauftragte

Die Compliance-Beauftragten sind dafür zuständig, die für die Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren und deren Einhaltung zu prüfen.

…ca 30 wesentliche Rollen, die in Informationssicherheit nach BSI Grundschutz involviert sind

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Aufgabe zum IT-Grundschutz

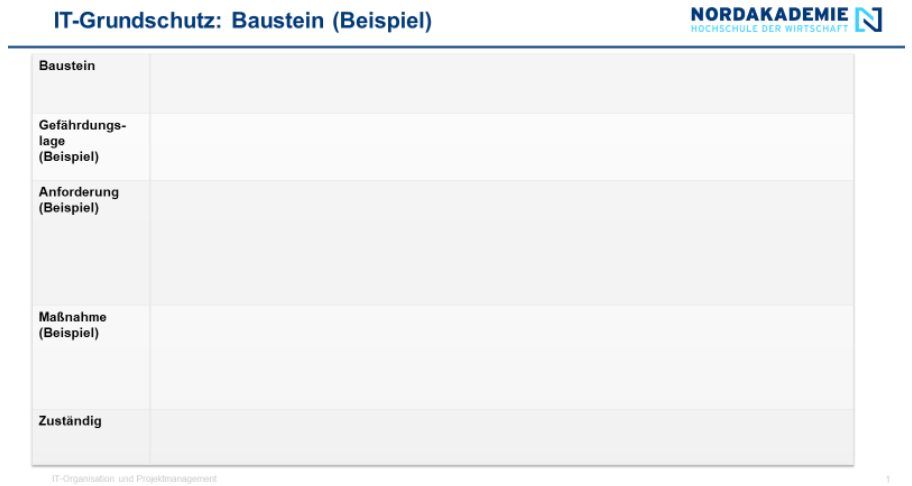
NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Gruppenarbeit:

1. Informationssammlung im Glossar des IT-Grundschutz-Kompendiums (dort ab Seite 35) zu folgenden Begriffen:
   - Informationsverbund
   - Modellierung
   - Strukturanalyse
   - Sicherheitsanforderung
   - Bausteine
   - Schutzbedarf
   - Zielobjekte

2. Die Begriffe sind in eine sinnvolle Reihenfolge zu bringen, die sich an das Vorgehen zur "Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung" gemäß BSI-Standard 200-2 (dort insbes. Kapitel 8) anlehnt.

3. Aus dem Grundschutz-Kompendium ist ein Baustein auszuwählen. Dieser ist in einem Steckbrief (gemäß Vorlage) zu beschreiben.
   Hinweis: Informationen zu den Bausteinen finden sich im Kompendium über das Inhaltsverzeichnis (ab S. 8), Informationen zu möglichen Maßnahmen finden sich zu vielen Bausteinen in den "Umsetzungshinweisen (2019)" , einzelne Aktualisierungen dazu auch hier.



IT-Grundschutz: Informationssammlung (Beispiel)

(Nr.) Informationsverbund

(Nr.) Modellierung

(Nr.) Strukturanalyse

(Nr.) Sicherheitsanforderung

(Nr.) Bausteine

(Nr.) Schutzbedarf

(Nr.) Zielobjekte

IT-Grundschutz: Baustein (Beispiel)

Baustein	
Gefährdungs-lage (Beispiel)	
Anforderung (Beispiel)	
Maßnahme (Beispiel)	
Zuständig	