
Inhaltsübersicht

1	Grundlagen der IT-Governance	1
2	Der Wertbeitrag der IT als Handlungsfeld der IT-Governance	55
3	Akteure der IT-Governance	121
4	Stakeholder als Handlungsfeld der IT-Governance	157
5	IT-Organisation als Handlungsfeld der IT-Governance	193
6	IT-Risiken als Handlungsfeld der IT-Governance	271
7	IT-Compliance als Handlungsfeld der IT-Governance	331
8	Data Governance	405
9	Standards und Normen der IT-Governance	441
	Anhang	481
A	Abkürzungen	483
B	Literaturverzeichnis	491
	Index	517

Inhaltsverzeichnis

1	Grundlagen der IT-Governance	1
1.1	Entwicklung der Corporate Governance	1
1.2	Definitionen für IT-Governance	5
1.3	IT-Governance nach Weill et al.	8
1.4	IT-Governance nach der ISO/IEC 38500	15
1.5	IT-Governance nach COBIT 2019	19
1.6	IT-Governance nach Van Grembergen/De Haes et al.	23
1.7	Verständnis von IT-Governance in diesem Buch	27
1.7.1	Vorüberlegungen	27
1.7.2	Darstellung unseres Verständnisses von IT-Governance ..	30
1.7.3	Prinzipien gemäß dem IT-Governance-Verständnis	34
1.8	Handlungsfelder für IT-Governance	40
1.8.1	Messung und Management des Wertbeitrags der IT im Rahmen der IT-Governance	40
1.8.2	Aufgaben und Verantwortlichkeiten der Akteure der Unternehmens-IT und ihre Positionierung in der Organisation	41
1.8.3	IT-Stakeholder als Adressaten der IT-Governance – Stakeholder in die Entwicklung der Unternehmens-IT einbeziehen	43
1.8.4	Organisation der Unternehmens-IT – interne und externe Anforderungen an die IT in Strukturen und Prozessen abbilden	44
1.8.5	IT-Risikomanagement – Managen von Unsicherheit durch Bewertung, Steuerung und Überwachung der Risiken	46
1.8.6	Compliance der Unternehmens-IT – Konformität mit gesetzlich-regulatorischen Vorgaben, IT-Standards und -Normen sowie internen IT-Richtlinien gewährleisten	48

1.8.7	Wert von Daten durch Data Governance sichern – Ziele, Verantwortlichkeiten und Rollen für ein erfolgreiches Datenmanagement festlegen	49
1.8.8	Standards und Normen der IT-Governance – bewährte Konzepte und Modelle für die Ausgestaltung der IT-Governance nutzen	51
1.9	Handlungsempfehlungen	53
2	Der Wertbeitrag der IT als Handlungsfeld der IT-Governance	55
2.1	Prioritäten, Trends und Herausforderungen	55
2.2	Wertbeitrag in wissenschaftlichen Studien und die Rolle der IT-Governance	61
2.3	Was bedeutet Wert und was ist der Wertbeitrag der IT?	65
2.3.1	Terminologie, Verfahren und Methoden	65
2.3.2	Grundlegendes Verständnis von »Wert« und Wertbeitrag der IT	67
2.3.3	Grundlegende Probleme und Herausforderungen bei der Ermittlung des Wertbeitrags	69
2.4	Messung und Messkonzepte für den Wertbeitrag der IT	72
2.4.1	Kostenorientierte Verfahren	72
2.4.2	Prozesskosten in Fach- und Geschäftsbereichen	74
2.4.3	Investitionsrechnung	74
2.4.4	Nutzwertanalyse	75
2.4.5	Weitere Verfahren im Überblick	77
2.4.6	Wert als »Nutzenbündel« (»Bundle of Benefits«-Ansatz) . .	77
2.5	Wertbeitrag und Wertbeitragsdimensionen	79
2.6	Konzepte zur Steuerung und Verbesserung des Wertbeitrags der IT	86
2.6.1	Business Case	86
2.6.1.1	Konzept und Grundlagen	86
2.6.1.2	Entwicklung eines Business Case	87
2.6.2	Business/IT-Alignment	95
2.6.2.1	Grundlagen und Definitionen	95
2.6.2.2	Das Strategic Alignment Model (SAM) und Erweiterungen	97
2.6.2.3	Alignment-Dimensionen und -Ebenen	100
2.6.2.4	Strategic Alignment Maturity Model (SAMM)	103
2.6.3	COBIT EDM02	109
2.7	Herausforderungen und Handlungsempfehlungen	115

3	Akteure der IT-Governance	121
3.1	Der Chief Information Officer	122
3.1.1	Stelle und Rolle des CIO	122
3.1.2	Beispiel für eine CIO-Organisation	130
3.2	Der Chief Digital Officer	133
3.2.1	Position und Aufgaben des Chief Digital Officer	133
3.2.2	Chief Digital Officer und Chief Information Officer	135
3.2.3	Der CDO in der bimodalen bzw. ambidextrischen IT ...	138
3.3	Gremien zur Steuerung und Überwachung der IT	141
3.3.1	Aufsichtsrat	141
3.3.2	Unternehmensleitung	145
3.3.3	Ausschüsse	149
3.4	Handlungsempfehlungen	154
4	Stakeholder als Handlungsfeld der IT-Governance	157
4.1	IT-Stakeholder als Adressaten der IT-Governance	157
4.1.1	Externe Akteure im Unternehmensumfeld	157
4.1.2	Stakeholder-Begriff	159
4.1.3	Verantwortung für Einbeziehung von IT-Stakeholdern ..	160
4.1.4	Beziehungen zwischen Unternehmens-IT und IT-Stakeholdern	162
4.1.5	Akteure in der Unternehmensumwelt	164
4.2	IT-Stakeholder	166
4.2.1	Unterscheidung zwischen externen und internen IT-Stakeholdern	166
4.2.2	Interne IT-Stakeholder	168
4.2.3	Externe IT-Stakeholder	173
4.3	Ziele der IT-Governance in Bezug auf die IT-Stakeholder	176
4.4	Abgrenzung zum IT-Stakeholder-Management	180
4.5	Konstitutive Entscheidungen für das IT-Stakeholder- Management	182
4.5.1	IT-Stakeholder-Identifizierung	182
4.5.2	IT-Stakeholder-Analyse	183
4.5.3	IT-Stakeholder-Einbindung	183
4.5.4	Qualifizierung für das IT-Stakeholder-Management	185

4.6	Überwachung des IT-Stakeholder-Managements	187
4.6.1	IT-Stakeholder-Identifizierung	187
4.6.2	IT-Stakeholder-Analyse	188
4.6.3	IT-Stakeholder-Einbindung	188
4.6.4	Kennzahlen für die Überwachung des IT-Stakeholder-Managements	189
4.7	Handlungsempfehlungen	190
5	IT-Organisation als Handlungsfeld der IT-Governance	193
5.1	Herausforderungen und Anforderungen an die IT-Organisation ..	193
5.1.1	Aktuelle Herausforderungen für die IT-Organisation	193
5.1.2	Gesetzlich-regulatorische Anforderungen an die Organisation der IT	196
5.2	Begriff und Umfang der IT-Organisation	199
5.3	Integration der IT-Funktion in die Unternehmensstruktur	203
5.3.1	Aufgaben, Stellen und Rollen der IT-Funktion	204
5.3.1.1	Aufgaben der IT-Abteilung	204
5.3.1.2	Rollen in der IT-Organisation	215
5.3.2	Aufbauorganisatorische Anbindung der IT-Abteilung ...	220
5.3.2.1	Grundformen der aufbauorganisatorischen Eingliederung der IT	220
5.3.2.2	Center-Konzepte für den IT-Bereich	223
5.3.3	Einfluss von Outsourcing auf die IT-Organisation	227
5.3.4	Integration der IT in das Unternehmen nach dem 3-Linien-Modell	236
5.4	IT-Prozesse	240
5.4.1	Struktur der IT-Prozesse nach COBIT 2019	240
5.4.2	Leistungssteuerung der IT-Prozesse nach COBIT 2019 ..	245
5.4.3	Priorisierung der Prozesse mittels Designfaktoren	247
5.5	Agile IT-Organisation	250
5.5.1	Agile IT aus Sicht der IT-Governance	250
5.5.2	Agile Aufbauorganisation	256
5.5.3	DevOps	259
5.5.4	Innovation Labs	263
5.6	Handlungsempfehlungen	265

6	IT-Risiken als Handlungsfeld der IT-Governance	271
6.1	Grundlagen für die Governance von IT-Risiken	272
6.1.1	Grundlagen in Gesetzen, Standards und Normen	272
6.1.2	Begriff des IT-Risikos	273
6.1.3	Systematik der IT-Risiken	274
6.2	IT-Risiken im Rahmen der IT-Governance	276
6.2.1	IT-Risiken in der Trias »IT-GRC«	276
6.2.2	IT-Risiken in der ISO/IEC 38500	277
6.2.3	Governance von IT-Risiken nach COBIT 2019	278
6.2.4	IT-Risiken als Teilmenge der Unternehmensrisiken	281
6.2.5	IT-Risiken im Rahmen des unternehmensweiten Risikomanagements	285
6.3	Wertbeitrag der Governance von IT-Risiken	287
6.4	Aufgabenbereiche der Governance von IT-Risiken	289
6.4.1	Struktur der Aufgabenbereiche	289
6.4.2	IT-Risikoziele	290
6.4.3	IT-Risikobewusstsein	291
6.4.4	IT-Risikokultur	293
6.4.5	Grundlegende IT-Risikoorientierung	295
6.4.6	IT-Risikostrategie und IT-Risikorichtlinie	296
6.4.7	IT-Risiko-Stakeholder	297
6.4.8	IT-Risikoorganisation	301
6.4.9	IT-Risikomanagementsystem	301
6.5	Organisation und Mechanismen des IT-Risikomanagements	302
6.5.1	Umfeld der IT-Risikoorganisation	302
6.5.2	IT-Risikomanagementprozess	304
6.5.2.1	Risikomanagementprozess nach DIN ISO 31000	304
6.5.2.2	Risikomanagementprozess nach COBIT 2019	306
6.5.2.3	Risikomanagementprozess nach IDW PS 981	308
6.5.2.4	Risikomanagementprozess nach DIIR Revisionsstandard Nr. 2	310
6.5.3	Strukturelle IT-Risikoorganisation	311
6.5.3.1	Organisationseinheiten	311
6.5.3.2	Rollen	313

6.6	IT-Risikomanagementsystem	314
6.6.1	IT-Risikomanagementsystem nach DIN ISO 31000	315
6.6.2	IT-Risikomanagementsystem nach IDW PS 981	319
6.6.3	IT-Risikomanagementsystem nach DIIR Revisionsstandard Nr. 2	320
6.6.4	Prüfung des IT-Risikomanagementsystems	322
6.6.4.1	Formen und Zielsetzung der Prüfung	322
6.6.4.2	Prüfung nach DIIR Revisionsstandard Nr. 2	323
6.6.4.3	Prüfung nach IDW PS 981	325
6.7	Handlungsempfehlungen	327
7	IT-Compliance als Handlungsfeld der IT-Governance	331
7.1	Grundlagen	331
7.1.1	Einordnung von IT-Compliance in die Governance	331
7.1.2	Treiber für IT-Compliance	332
7.1.3	Wertbeitrag der IT-Compliance	333
7.2	Methodische Grundlagen	336
7.2.1	Begriff	336
7.2.2	Rahmenwerke für IT-Compliance	339
7.2.2.1	COBIT 2019	339
7.2.2.2	ISO 37301	341
7.2.2.3	IDW PS 980 n.F.	343
7.2.2.4	Weitere Entwicklung der Rahmenwerke	345
7.3	Regelwerke für IT-Compliance	347
7.3.1	Klassifizierung der Regelwerke	347
7.3.2	Rechtliche Vorgaben	350
7.3.2.1	Gesetze	350
7.3.2.2	Rechtsprechung	353
7.3.2.3	Rechtsverordnungen	353
7.3.2.4	Verwaltungsvorschriften	354
7.3.3	Verträge	356
7.3.4	Unternehmensinterne Regelwerke	359
7.3.5	Unternehmensexterne Regelwerke	360
7.4	Auswahl von relevanten Regelwerken	361
7.4.1	Bestimmung des Compliance-Portfolios	361
7.4.2	Konsolidierung von Regelwerken	362
7.4.3	Mapping	366

7.5	Gestaltungselemente der IT-Compliance	367
7.5.1	Einordnung in die Corporate Compliance	367
7.5.2	IT-Compliance-Kultur	368
7.5.3	IT-Compliance-Ziele	370
7.5.4	IT-Compliance-Risiken	374
7.5.5	IT-Compliance-Programm	376
7.5.6	IT-Compliance-Organisation	379
7.5.6.1	Einflussfaktoren	379
7.5.6.2	Organisationsformen	380
7.5.6.3	IT-Compliance-Manager	384
7.5.6.4	IT-Compliance-Prozess	386
7.5.7	IT-Compliance-Kommunikation	390
7.5.8	IT-Compliance-Überwachung	391
7.6	Nachweis der IT-Compliance	392
7.6.1	Prüfung nach IDW PS 980 n.F.	392
7.6.2	Prüfungen nach IDW PS 860	394
7.6.3	Prüfung nach IDW PS 951 n.F.	400
7.7	Handlungsempfehlungen	401
8	Data Governance	405
8.1	Data Governance im Rahmen der IT-Governance	405
8.2	Begriff der Data Governance	408
8.3	Wertbeitrag und Ziele von Data Governance	415
8.4	Organisation der Data Governance	419
8.5	Normen und Standards für Data Governance	423
8.5.1	Data Governance nach DAMA-DMBOK	424
8.5.1.1	Der »Data Management Body of Knowledge«	424
8.5.1.2	Zielsetzung und Prinzipien von Data Governance	425
8.5.1.3	Data Governance und Datenmanagement	426
8.5.1.4	Prozess der Data Governance	426
8.5.1.5	Akteure der Data Governance	430
8.5.1.6	Bewertung des DAMA-DMBOK	431
8.5.2	Data Governance nach COBIT 2019	431
8.5.2.1	Managementziel APO14	431
8.5.2.2	Governance-Ziel EDM04	432
8.5.2.3	Bewertung von COBIT 2019	434

8.5.3	Data Governance nach ISO/IEC 38505-1 und -2	434
8.5.3.1	ISO/IEC 38505-1	434
8.5.3.2	ISO/IEC 38505-2	437
8.6	Handlungsempfehlungen	439
9	Standards und Normen der IT-Governance	441
9.1	Frameworks, Standards und Normen	441
9.1.1	Zur Begrifflichkeit	441
9.1.1.1	Standard	442
9.1.1.2	Norm	443
9.1.1.3	Framework	444
9.1.2	Normungsorganisationen	445
9.1.3	Allgemeiner Nutzen aus IT-Normen und -Standards	447
9.2	Für IT-Governance relevante IT-Normen	451
9.2.1	Die Normenreihe ISO/IEC 3850x	451
9.2.2	Die Norm ISO/IEC 27014	456
9.3	COBIT 2019 als Standard für die IT-Governance	460
9.3.1	Struktur der COBIT-Dokumente	460
9.3.2	IT-Governance-System nach COBIT 2019	461
9.3.3	IT-Governance und IT-Managementziele	463
9.3.4	IT-Prozesse	466
9.3.5	Zielkaskade	476
9.4	Handlungsempfehlungen	478
	Anhang	481
A	Abkürzungen	483
B	Literaturverzeichnis	491
	Index	517