

IT-Unternehmensarchitektur

Von der Geschäftsstrategie zur
optimalen IT-Unterstützung

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhaltsübersicht

1	Einleitung und Überblick	1
2	Was ist IT-Unternehmensarchitektur?	23
3	Zielmuster	45
4	Managementprozessmuster	69
5	Sichten und Informationsmodelle	179
6	Compliance	207
7	Cybersicherheitsarchitektur	231
8	IT-Risikomanagement	317
9	Makro-Architekturmuster	327
10	Frameworks für IT-Unternehmensarchitektur	349
11	IT-Management-Frameworks	375
12	Werkzeuge für Enterprise Architecture Management	387
13	Lean und Agile EAM	411
14	Pragmatische Vorgehensweisen	423
15	Einführungspfade für IT-Unternehmensarchitektur	461
16	Ausblick	473
Anhang		483
A	Checkliste für Richtlinien, Vorstudien und Architekturdokumente	485
B	Textauszüge	491
C	Abkürzungsverzeichnis	497
D	Glossar	503
E	Literatur	509
	Stichwortverzeichnis	523

Inhaltsverzeichnis

1	Einleitung und Überblick	1
1.1	Motivation des Buches	3
1.2	Struktur des Buches	6
1.3	Wer sollte dieses Buch lesen und warum?	11
1.3.1	Eine Frage der Unternehmensgröße?	12
1.3.2	IT-Unternehmensarchitekten	13
1.3.3	Verantwortliche für Business Development	15
1.3.4	IT-Vorstände, CIOs und CDOs	15
1.3.5	Softwarearchitekten	16
1.3.6	Alle anderen IT-Mitarbeiter	17
1.3.7	Studierende	17
1.4	Wie können Sie dieses Buch lesen?	18
1.5	Einige Besonderheiten	18
1.5.1	Sprache: Deutsch	18
1.5.2	Verwendung von Wikipedia-Definitionen	19
1.6	Was sich seit der ersten Auflage geändert hat	19
2	Was ist IT-Unternehmensarchitektur?	23
2.1	Das Substantiv: Unternehmensarchitektur als Struktur	24
2.1.1	Geschäftsarchitektur	26
2.1.1.1	Geschäftsarchitektur in TOGAF 10 th Edition	27
2.1.1.2	Geschäftsarchitektur nach Reynolds	29
2.1.1.3	Geschäftsmodelle (Business Models)	30
2.1.1.4	Digitale Geschäftsmodelle	32
2.1.1.5	Enterprise Architecture nach Intersection Group ..	34
2.1.2	IT-Unternehmensarchitektur	36
2.2	Die Tätigkeit: Unternehmensarchitektur als Management	37
2.3	Musterbasierter Ansatz für IT-Unternehmensarchitektur	39

3	Zielmuster	45
3.1	Business-IT-Alignment	48
3.1.1	Bedeutung	49
3.1.2	Dimensionen	50
3.1.3	Zwischenbilanz	53
3.2	Verbesserung der Ertragskraft und Kostenmanagement	53
3.2.1	Verbesserung der Ertragskraft des Business	54
3.2.2	Reduktion von IT-Kosten	56
3.3	Optimierung mit Sourcing-Strategien	61
3.4	Verbesserung Time-to-Market	62
3.5	Verbesserung Kundenzufriedenheit	65
3.6	Reduktion von Heterogenität	65
3.7	Bewältigung von Fusionen	67
3.8	Compliance, Sicherheit und Risikomanagement	67
4	Managementprozessmuster	69
4.1	IT-Strategieentwicklung	73
4.1.1	Was ist eine Strategie?	73
4.1.2	Ein kurzer Blick auf den Strategieprozess	75
4.1.3	Wozu sollte eine IT-Strategie Aussagen machen?	75
4.1.4	Wo bleibt hier bitte die Digitalisierung?	79
4.1.5	Herausforderungen bei der Umsetzung in der Praxis	80
4.1.6	Der Maxime-Prozess	82
4.2	Business-IT-Alignment herstellen mit Capabilities	83
4.2.1	Was sind Capabilities?	84
4.2.2	Investitionssteuerung mit Capabilities	85
4.2.3	Wie kommt man zu einem sinnvollen Katalog von Capabilities?	87
4.2.4	Wie kommt man zu den Bewertungen der Capabilities? ...	91
4.2.5	Zwischenbilanz: Warum helfen Capabilities bei der strategischen Ausrichtung einer Anwendungslandschaft? ..	91
4.2.6	Optimierung des Sourcings einer Anwendungslandschaft mit Capabilities	92
4.2.7	Vergleich von Anwendungen mit Footprints	94
4.3	Management des Anwendungsportfolios	95
4.3.1	Grundlegende Begriffe zum Management des Anwendungsportfolios	96
4.3.2	Management des Anwendungsportfolios als zyklischer Prozess	98

4.4	Erfassung der Ist-Anwendungslandschaft	100
4.4.1	Umfang	101
4.4.2	Typische Attribute für eine minimale Befüllung	101
4.4.3	Erfassung von Schnittstellen: Ja oder Nein?	102
4.4.4	Keyvisual für die Anwendungslandschaft	104
4.4.5	Tipps und Tricks	105
4.5	Auswertungen des Anwendungsportfolios	106
4.6	Anwendungslandschaft, Metriken und Dashboards	111
4.7	Strategische Bebauungsplanung	114
4.7.1	Grundsätzliches Vorgehen	115
4.7.2	Erfassen der Anforderungen (Scoping)	117
4.7.3	Analyse und Bewertung (Analysis)	118
4.7.4	Erarbeiten der Zielbebauung (Design)	119
4.7.5	Abstimmung (Design)	119
4.7.6	Maßnahmenplanung (Plan Implementation)	120
4.7.7	Zusammenfassung der strategischen Bebauungsplanung	120
4.8	Management eines Serviceportfolios	121
4.9	Managed Evolution	126
4.10	Etablieren eines IT-Governance-Systems	130
4.10.1	Was ist IT-Governance?	131
4.10.2	Hierarchie von Governance-Systemen	133
4.10.3	Stile von IT-Governance	133
4.10.4	Hinzunahme des Unternehmenstyps	136
4.11	Architektur-Governance	142
4.11.1	Aufbauorganisation der IT-Governance und Architektur-Governance	143
4.11.2	Entwicklung und Durchsetzung von Richtlinien	149
4.11.3	Monitoring des Projektportfolios	154
4.11.4	Projektbegleitung	157
4.11.5	Über Reviews im Rahmen der Projektbegleitung	161
4.12	SOA-Governance	165
4.12.1	Schichten	166
4.12.2	Operationale und technische SOA-Governance	168
4.12.3	Business-Motivation für SOA	170
4.13	Management von Fusionen	171
4.13.1	Die Leiter der Integration	171
4.13.2	Grundmuster von Anwendungskonsolidierungen	173
4.14	Reduktion von Heterogenität	177

5	Sichten und Informationsmodelle	179
5.1	Softwarekartografie als Grundlage der Systematisierung	181
5.2	Typen von Softwarekarten	182
5.2.1	Clusterkarten	183
5.2.2	Prozessunterstützungskarten	184
5.2.3	Intervallkarten	186
5.2.4	Karten ohne Kartengrund	187
5.3	Viewpoints und Viewpoint-Patterns	188
5.3.1	Viewpoints in ISO/IEC/IEEE 42010 und TOGAF	188
5.3.2	Viewpoint-Patterns	190
5.3.3	Diskussion der Pattern-Qualität	192
5.4	Informationsmodelle	192
5.4.1	Das TOGAF Content Metamodel	194
5.4.2	Hybride Wikis als Repository für IT-Unternehmensarchitektur	195
6	Compliance	207
6.1	Was ist »Compliance«?	207
6.2	IT-Compliance im Kontext von Enterprise Compliance	210
6.3	Exemplarische Compliance-Themen für die IT	211
6.3.1	Basel II, III und IV	212
6.3.2	Solvency II	216
6.3.3	Der Sarbanes-Oxley Act (SOX)	217
6.4	KonTraG	222
6.5	Aufbewahrungsfristen	223
6.5.1	E-Mails sind archivierungspflichtig	223
6.5.2	Stilllegung von DV-Systemen	224
6.6	COBIT und Compliance	225
6.6.1	Beispiel aus APO02 – Managen der Strategie	226
6.6.2	Beispiel aus APO03 – Managen der Unternehmensarchitektur	227
6.7	Der Clinger-Cohen Act	228

7	Cybersicherheitsarchitektur	231
7.1	Zielmuster	233
7.1.1	Zielmuster: Bedrohungen abwehren	234
7.1.1.1	Schutzbedarfsanalyse	236
7.1.1.2	Bedrohungsanalyse	237
7.1.1.3	Umfassender Schutz	244
7.1.2	Zielmuster: Compliance herstellen	245
7.1.2.1	Identifikation der Anforderungen	245
7.1.3	Zielmuster in Einklang bringen	248
7.1.4	Zusammenhang mit dem Risikomanagement	250
7.2	Managementprozessmuster	251
7.2.1	Sicherheitsstrategie	251
7.2.2	Cybersicherheitsparadigmen	253
7.2.2.1	Defend the Perimeter	253
7.2.2.2	Assume Breach	253
7.2.2.3	Defense in Depth	255
7.2.2.4	Jeder schützt sich selbst	255
7.2.2.5	Betreibbarkeit geht vor Sicherheit	255
7.2.2.6	Security/Privacy by Design	256
7.2.3	Organisation der Cybersicherheit	256
7.2.3.1	Modell: Zentrale IT	258
7.2.3.2	Modell: Dezentrale IT	259
7.2.3.3	Modell: One IT-Team	260
7.2.3.4	Mischformen	261
7.2.3.5	Sicherheit auf Projektebene	261
7.2.4	Umsetzung des ISO-2700x-Standards	262
7.2.4.1	Überblick	262
7.2.4.2	Einführung ISMS	264
7.2.5	Prüfung der Sicherheit	267
7.2.5.1	Audits	267
7.2.5.2	Penetrationstests/Redteaming	270
7.2.5.3	Outside-In Checks	271
7.2.5.4	Schwachstellenscans	271
7.2.5.5	Awareness-Trainings	272
7.2.5.6	Phishing-Tests	272
7.2.6	Umgang mit Notfällen und Krisen	272
7.2.6.1	Reaktive Sicherheit als Aufgabe der CISO-Organisation	272
7.2.6.2	Vorbereitungen für das Alarmstufenmanagement	277
7.2.6.3	Tatorthygiene für Administratoren	278
7.2.6.4	Alarmstufe Gelb: 100 % Wachsamkeit	280
7.2.6.5	Alarmstufe Orange: Schilde hoch, Waffen bereit machen	282
7.2.6.6	Alarmstufe Rot: Krise	284

7.3	Lösungsmuster auf Infrastrukturebene	286
7.3.1	Unternehmensweite Sicherheitssegmente	286
7.3.2	Aufbau unternehmensweiter Sicherheitsinfrastrukturen	288
7.3.2.1	Phishing-Schutz	288
7.3.2.2	Client Hardening	289
7.3.2.3	Zugänge von außen kontrollieren	290
7.3.2.4	Offline-Backup	290
7.3.2.5	Domäne schützen	291
7.3.2.6	Erkennung von Angriffen im internen Netz	292
7.3.2.7	Patchmanagement	293
7.3.2.8	Virtualisierungsinfrastruktur	294
7.3.2.9	Cloud-Umgebungen	294
7.3.2.10	Zentrales Logging und Protokollierung	294
7.3.3	Sicherheit betreiben	295
7.4	Lösungsmuster auf Applikationsebene	296
7.4.1	Konzeptionelle Architekturmuster	297
7.4.1.1	Klare Sicherheitsverantwortung	297
7.4.1.2	Sicherheitsorientierte Segmentierung	298
7.4.1.3	Sichere Modellierung der fachlichen Schnittstellen	298
7.4.1.4	Zentrale Infrastrukturen	299
7.4.1.5	Applikationsinternes Software Lifecycle Management	300
7.4.1.6	Defense in Depth	301
7.4.1.7	Sicherheitsmanagement über den Lifecycle hinweg	301
7.4.1.8	Compliance	302
7.4.2	Funktionale Architekturmuster	303
7.4.2.1	Rollen und Rechte	303
7.4.2.2	Logging	305
7.4.2.3	Privacy by Design, Privacy by Default	305
7.4.2.4	Updates, Apps, Sandboxing	306
7.4.3	Nicht funktionale Architekturmuster	306
7.4.3.1	Modellierung von Schutzzonen	307
7.4.3.2	Risikobewusste Einbindung von Anwendungen in die Netzwerkinfrastruktur	307
7.4.3.3	Verschlüsselung auf Applikationsebene	309
7.4.3.4	Verschlüsselung auf Netzwerkebene	309
7.4.3.5	Einbindung in Infrastruktur- und Betriebssicherheit	310
7.4.3.6	Sicherheitsbewusstes Codedesign	311
7.4.3.7	Sicherheitstechnisch korrekte Konfiguration	312
7.4.4	Testen	313
7.4.5	Dokumentation & Vollständigkeitscheck	314
7.5	Zusammenfassung	315

8	IT-Risikomanagement	317
8.1	Was ist Risikomanagement?	320
8.2	Management von Risiken mit Total Risk Profiling	322
8.3	Risikoregister für Anwendungen	324
9	Makro-Architekturmuster	327
9.1	Blueprints und Architekturrichtlinien	328
9.1.1	Abstützen auf Standards	329
9.1.2	Beschreibungsmittel	330
9.1.3	Marchitecture: der Marketingaspekt	330
9.2	Beispiel: Facharchitektur für Versicherungen	331
9.2.1	Beispiel zur Beschreibungstiefe einer Facharchitektur	333
9.2.2	Einsatz und Nutzen einer Facharchitektur	334
9.2.3	Abgrenzung zu Informationsarchitekturen	335
9.2.4	Verwendung der Facharchitektur für die Bebauungsplanung	335
9.3	Beispiele für technische Architekturmuster	336
9.3.1	Beispiel: SOA	337
9.3.2	Beispiel: Blueprint für Internetanwendungen	342
9.3.3	Beispiel: Microservices und REST	344
10	Frameworks für IT-Unternehmensarchitektur	349
10.1	Ordnungsrahmen für EAM- und IT-Management-Frameworks ...	350
10.2	TOGAF 10 th Edition	355
10.2.1	Die Sicht von TOGAF 10 th Edition auf IT-Unternehmensarchitektur	357
10.2.2	Der Kern von TOGAF: die »Architecture Development Method« (ADM)	359
10.2.3	Abgleich von TOGAF mit Prozessclustern der IT-Unternehmensarchitektur	362
10.2.4	Abdeckung weiterer Aufgabenbereiche durch TOGAF ...	366
10.2.5	Sonstige nützliche Aspekte von TOGAF	368
10.2.6	Künftige Versionen von TOGAF	370
10.3	Zachman-Framework	371

11	IT-Management-Frameworks	375
11.1	COBIT	376
11.1.1	Grobstruktur des COBIT-Prozessmodells	378
11.1.2	Nutzen von COBIT für IT-Unternehmensarchitekten	382
11.2	ITIL	382
11.2.1	ITIL 3	383
11.2.2	ITIL 4	384
12	Werkzeuge für Enterprise Architecture Management	387
12.1	Abwägungen beim Werkzeugeinsatz	389
12.2	Umfang eines integrierten IT-Planungswerkzeugs	392
12.2.1	Zu unterstützende Prozesse der IT-Unternehmensarchitektur	394
12.2.2	Sonstige Prozesse des IT-Managements	397
12.2.3	Schnittstellen eines IPIT zu anderen Arten von Werkzeugen	399
12.2.4	Weitere funktionale Anforderungen an IPITs	400
12.2.5	Nicht funktionale Anforderungen an IPITs	401
12.3	Möglicher Umfang von Planungswerkzeugen	403
12.3.1	Werkzeuge mit maximalem Umfang: das umfassende Informationssystem für die IT-Funktion?	403
12.3.2	Werkzeuge mit realistischem Funktionsumfang: IPIT	404
12.3.3	Werkzeuge mit mittlerem Funktionsumfang: Aufsätze auf bestehenden Lösungen	404
12.3.4	Werkzeuge mit geringem Funktionsumfang: Ad-hoc-Werkzeuge nur für Bebauungsplanung	405
12.4	Herkunft der Werkzeuge	406
12.5	Marktsituation	408
13	Lean und Agile EAM	411
13.1	Lean und IT-Unternehmensarchitektur	412
13.1.1	Lean-Prinzipien	413
13.1.2	Lean auf Prozesse der IT-Unternehmensarchitektur anwenden	414
13.2	Die Tätigkeit: agile Praktiken auf EAM-Prozesse anwenden	415
13.2.1	Agiles Manifest und agile Prinzipien	415
13.2.2	Ableich Lean und Agile	417
13.3	Das Substantiv: agile Softwarearchitektur	419

14	Pragmatische Vorgehensweisen	423
14.1	Angemessenes Budget für IT-Unternehmensarchitektur	423
14.1.1	Zahlt sich IT-Unternehmensarchitektur aus?	424
14.1.2	Wie groß sollte eine Architekturgruppe sein?	429
14.2	Wie viel Ordnung muss sein?	430
14.2.1	Wie sorgt man für die Reduktion von Komplexität?	430
14.2.2	Wie viel Ordnung ist gut? Gibt es zu viel Ordnung?	431
14.3	Gefahren für Unternehmensarchitekten	438
14.3.1	Exkurs: Organisationsmuster für die IT-Funktion	439
14.3.2	Auf die Beschaffungsseite fixierter IT-Vorstand	444
14.3.3	Organigramm alten Stils	444
14.3.4	Hierarchiedenken	445
14.3.5	Chicken Race	445
14.3.6	Mangelnde Offenheit	447
14.3.7	Verzetteln: keine klare Strategie	447
14.3.8	Inkonsequenz	448
14.4	Zusammenarbeit mit Lösungsarchitekten	449
14.4.1	Warum macht der IT-Unternehmensarchitekt nicht meine Projektarchitektur?	449
14.4.2	Das Kostendilemma der Wiederverwendung	452
14.5	Tipps und Tricks	453
14.5.1	Architekturtickets	453
14.5.2	Radar-Chart-Methode	455
14.5.3	Chefmanagement	457
15	Einführungspfade für IT-Unternehmensarchitektur	461
15.1	IT-Unternehmensarchitektur für Großunternehmen	461
15.2	Einführungspfade für IT-Unternehmensarchitektur mit und ohne Topmanagement-Unterstützung	462
15.3	Wege in Konzernen mit dezentralen IT-Einheiten	469
16	Ausblick	473

Anhang	483	
A	Checkliste für Richtlinien, Vorstudien und Architekturdokumente	485
A.1	Wer kann diese Checkliste verwenden und warum?	485
A.2	Zu Beginn	486
A.2.1	Reviewen ist eine Dienstleistung für den Autor	486
A.2.2	Schreiben ist eine Dienstleistung für den Leser	487
A.3	Kontrollfragen	487
A.3.1	Kontrollfragen zur Geschichte, die das Dokument wiedergibt	487
A.3.2	Formalia	489
B	Textauszüge	491
B.1	Auszug SOX Sections 302 und 404	491
B.2	Auszug AO (Abgabenordnung)	493
C	Abkürzungsverzeichnis	497
D	Glossar	503
E	Literatur	509
	Stichwortverzeichnis	523