

IT-Governance

als Basis strategischer IT-Steuerung,
Cloud-Governance und dem erfolgreichen
Management von Cyber-Risiken

Wolfgang Gaess

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

ISBN 978-3-8005-1857-1

dfv Mediengruppe

© 2023 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main
www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Druck: WIRMachenDRUCK GmbH, Backnang

Printed in Germany

Vorwort

Wir haben Stunden miteinander verbracht - und um die Ecke gedacht (Tocotronic – Um die Ecke [gedacht])

Die derzeit stattfindende **Technologische Transformation** vollzieht sich in Gestalt **Disruptiver Technologien** wie u. a. **Cloud** und **Künstlicher Intelligenz** sowie neuer Methoden wie **Agilem Projektmanagement** und dem Wandel hin zu **datengetriebenen Organisationen**. Der sich rasant ändernde Wettbewerb, mit teils marktfremden Akteuren auf „etablierten“ Märkten (u. a. BigTechs) sowie sich ständig ändernden Bedrohungslagen, erfordert kontinuierliche Analyse und planerische Anpassung. Diese Aufgaben erfüllt eine IT-Governance. Nur mit dadurch **konkretisierten und operationalisierten** Zielwerten und einer Zielerreichungsmessung wird auf Basis einer IT-Strategie wirklich gesteuert.

In der Realität hat sich bisher jedoch meist das Prinzip Wildwuchs durchgesetzt. Systemlandschaften sind Zufallsprodukt **auditgetriebenen Durchhangelns**. **Fehlender Durchblick** und **dürftige Dokumentation** sind zwangsläufige Begleitmangelercheinungen. Das hat aber nicht nur Auswirkung auf die Performanz der Kernfunktionen der IT. Vielmehr ist bei solchen Unzulänglichkeiten auch kein ordnungsgemäßes IT-Risikomanagement möglich. Beispielsweise müssen Informationsrisiken bzw. Datenschutzrisiken etc. über Geschäftsprozesse und Applikationslandschaften **nachvollziehbar und vollständig** erfasst werden – ehe sie gesamtlich bewertet über eine Configuration Management Database (CMDB) auf die Ebene der Infrastruktur vererbt werden. Dies sind **Grundlagen** für ein **belastbares Internes Kontrollsystem (IKS)** und **Non Financial Risks (NFR)** (bzw. OpRisk¹). Themen, die mithin durch die KRITIS-Verordnung, die zunehmenden Zertifizierungserfordernisse wie TISAX² oder nach ISO sowie anerkannte Prüfungsstandards wie ISAE³ (bzw. IDW PS⁴) mittlerweile **in allen Lieferketten** angekommen sind.

Die durch IT-Governance geschaffenen Leitlinien, Strukturen und Vorlagen **erleichtern die Arbeit** in und mit der IT. Die hierdurch **geschaffene Akzeptanz** steigert die Einhaltung der Vorgaben und erzeugt dadurch eine **Verbesserung des gesamtheitlichen IT-Betriebs** in Form von **Effizienzen und minimierten Risiken**. Es bewirkt im Nebeneffekt auch **höhere IT-Compliance**, die branchenübergreifend zunehmend von Wirtschaftsprüfern und In-

1 Operationelle Risiken.

2 Zertifizierungsstandard in der Automobilindustrie.

3 International Standard on Assurance Engagements.

4 Institut der Wirtschaftsprüfer Prüfungsstandards.

Vorwort

terner Revision erwartet wird. Für regulierte Unternehmen wird im Nebeneffekt der Nachweis für **Regulierungs-Compliance** geschaffen.

Die Erkenntnisse dieses Buches wurden in der Finanzbranche gewonnen und erfolgreich in der Praxis verprobt. Die **Finanzbranche eilt** bei Themen wie **Cyberisiken** sowie den **unterstützenden Ordnungsthemen** aufgrund ihres **hohen Regulierungsgrades bzw. der Regulierungsdichte anderen Industrien voraus** (insbesondere in Form von MaRisk⁵ und BAIT⁶ sowie den Feststellungen in den Prüfungsberichten der Finanzaufsicht).

Als Ursache des besonders hohen Regulierungsgrades in der Finanzbranche kann u. a. noch immer die Finanzkrise in den Jahren 2007/2008 herangezogen werden. Der Zusammenbruch der Silicon Valley Bank, Signature Bank und First Republic sowie der Credit Suisse im Jahr 2023 verleiht der Finanzregulierung neuen Nachdruck. Spätestens mit der **KRITIS-Verordnung** zeigte sich aber, dass auch andere Branchen von hoheitlicher Seite (hier der kritischen Infrastruktur) als **besonders schützenswert eingestuft** werden und mit Regulierung von hoheitlicher Seite Mindeststandards durchgesetzt werden.

Die in der Finanzbranche gewonnenen Erfahrungen und Erkenntnisse werden regelmäßig – leicht zeitlich versetzt – als „Good Practice“ in der **„Light Version“** in andere Industriestandards übernommen. Diese Entwicklung hat guten Grund. Gerade die IT-Vorgaben in der Finanzbranche sind meist keineswegs allein auf den Finanzbereich gemünzt (das wären eher die fachlichen Vorgaben für Kreditvergabe, Scoring etc.). Vielmehr handelt es sich um **allgemeingültige und sinnvolle Anforderungen zur Härtung des ganzheitlichen und integrierten IT-Risikomanagements**, was mittelbar mit der Stärkung der IT-Organisation, des IT-Betriebs und der IT-Informationssicherheit einhergeht. Die Verwaltungsanweisungen werden unter maßgeblicher Beiziehung des Bundesamtes für Sicherheit in der Informationstechnik⁷, von Wirtschaftsprüfern, IT-Experten sowie weiterer maßgeblicher kompetenter Akteure ausgearbeitet.

Lars Weimer, Dr. Christoph Capellaro, Dr. Franz Thiel, Christoph Becker, Olivia Nowak, Colin Herrmann, Tilman Friedrich und Nils Rasche haben dieses Buchvorhaben unterstützt und möglich gemacht. Ihnen ist an dieser Stelle herzlich gedankt.

Wolfgang Gaess

⁵ Rundschreiben 10/2021 (BA); Mindestanforderungen an das Risikomanagement – MaRisk.

⁶ Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021; Bankaufsichtliche Anforderungen an die IT.

⁷ BSI Standards.

Inhaltsverzeichnis

Vorwort	V
Abkürzungsverzeichnis	XIII
Abbildungsverzeichnis	XV
Tabellenverzeichnis	XVI
Erläuterung und Übersicht	1
Teil I: Organisation	3
1. Begriffsdefinition & Verständnis	3
1.1 Aufbau- und Ablauforganisation	4
1.2 Der richtige Blickwinkel	7
1.3 Gesellschaftsrechtlicher Blickwinkel	8
1.4 Organisatorischer Blickwinkel	9
1.5 Organisationsmodell	9
1.6 Implementierungsstrahl	11
1.7 Checkliste	11
2. Prozesshaus	12
2.1 Implementierungsstrahl	14
2.2 Checkliste	15
3. Methodik, Prinzipien und Leitlinien	15
3.1 Anwendbare Standards	15
3.2 Einsatz von Standards	16
3.3 Three Lines of Defense Modell	17
3.4 Risikoorientierung	19
3.5 Good-Practice-Standards	20
3.6 Implementierungsstrahl	20
3.7 Checkliste	21
4. Rollen und Beauftragte	21
4.1 Implementierungsstrahl	22
4.2 Checkliste	23
5. Gremien	23
5.1 Gremien allgemein	23
5.2 Implementierungsstrahl	24
5.3 Checkliste	25
6. Funktionen und Abteilungen	25
6.1 Implementierungsstrahl	27
6.2 Checkliste	27
7. Anwendbare Gesellschaften	27
7.1 Unterschiedlicher Regelungsbedarf	27
7.2 Implementierungsstrahl	28

Inhaltsverzeichnis

7.3	Checkliste	29
8.	Berichterstattung	29
8.1	Vorgaben an die Berichterstattung	29
8.2	Berichtsinhalte	30
8.3	Übersicht Berichterstattung	30
8.4	Implementierungsstrahl	31
8.5	Checkliste	31
Teil II: Kernthemen		32
1.	IT-Risikomanagement	32
1.1	Arten von Risiken in der IT	33
1.2	Ableitung übergeordnetes Risikomanagement	36
1.3	Vorgehensweise	36
1.4	Non-Financial-Risks oder OpRisk	37
1.5	Überwachung	37
1.6	Dokumentation	37
1.7	Implementierungsstrahl	38
1.8	Checkliste	39
2.	IT-Servicemanagement	39
2.1	IT-Servicemanagement als Supportprozess	40
2.2	IT-Servicemanagementgedanke als Leitbild	40
2.3	Definitionen von KPIs	42
2.4	Implementierungsstrahl	43
2.5	Checkliste	44
3.	Rechtsradar	44
3.1	Identifizierung relevanter Änderungen	45
3.2	Implementierungsstrahl	46
3.3	Checkliste	47
4.	Informationsmanagement	47
4.1	Informationsverbund	48
4.2	Strukturanalyse	50
4.3	Informationsrisikomanagement	50
4.4	Informationsmanagement	54
4.5	Wesentlichkeit oder Geschäftskritikalität	57
4.6	Implementierungsstrahl	59
4.7	Checkliste	60
5.	CMDB & IT-Assetmanagement	60
5.1	Anwendungsliste	61
5.2	Individuelle Datenverarbeitung (IDV)	61
5.3	Hardwareliste	61
5.4	CMS (Configuration-Management-System)	62
5.5	Implementierungsstrahl	63
5.6	Checkliste	64

Inhaltsverzeichnis

6. Ressourcenmanagement	64
6.1 Ressourcen- und Kostenmanagement	65
6.2 Implementierungsstrahl	67
6.3 Checkliste	68
7. IT-Compliance	68
7.1 Inhalt und Auftrag	69
7.2 Ausgestaltung eines CompMS	71
7.3 Meldepflichten	72
7.4 Implementierungsstrahl	73
7.5 Checkliste	74
8. Data-Governance	74
8.1 Definition	75
8.2 Entwicklung von Data-Governance	76
8.3 Einzelne Aufgaben der Data-Governance	79
8.4 Rollen und Verantwortlichkeiten	80
8.5 Kontrollen	80
8.6 Archivierung und Löschung	81
8.7 Testen mit Echtdateien	82
8.8 Implementierungsstrahl	84
8.9 Checkliste	85
9. IT-Architektur	85
9.1 Architekturmanagement	86
9.2 Mindestergebnisse aus der IT-Architektur	86
9.3 Datenarchitekturmanagement	89
9.4 Implementierungsstrahl	90
9.5 Checkliste	91
10. Strategische Entwicklung der IT	91
10.1 IT-Strategie	91
10.2 Inhaltliche Ausgestaltung	92
10.3 Weitere Themen	92
10.4 Aktualisierung der IT-Strategie	92
10.5 Implementierungsstrahl	94
10.6 Checkliste	95
Teil III: Schnittstellenthemen	96
1. Internes Kontrollsystem und Kontrollplan	96
1.1 Ziele	96
1.2 Kontrolldefinition	98
1.3 Risikoanalyse	98
1.4 Prozessrisikofilter (Wesentlichkeitsfilter)	99
1.5 Schlüsselkontrollen	99
1.6 Qualitätskontrollen	100
1.7 IT-Kontrollplan	101

Inhaltsverzeichnis

1.8	Implementierungsstrahl	103
1.9	Checkliste	104
2.	Qualitätsmanagement	104
2.1	Abgrenzung zu anderen Themen	104
2.2	Qualitätsüberwachung	105
2.3	Kontinuierliche Verbesserung der Services	106
2.4	Implementierungsstrahl	107
2.5	Checkliste	108
3.	IT-Auslagerungsmanagement	108
3.1	Auslagerungs-Governance	110
3.2	Risikoanalyse	111
3.3	Vertrag, SLAs, Anhänge & Templates	111
3.4	Providersteuerung	114
3.5	Organisationspflichten der Dienstleister	114
3.6	Industriespezifische Organisationspflichten	115
3.7	Grund-Organisationspflichten	115
3.8	Servicebezogene Organisationspflichten	116
3.9	Implementierungsstrahl	117
3.10	Checkliste	118
4.	Cloud-Governance & Cloud Compliance	118
4.1	Entwicklung von Cloud	118
4.2	Technologische Transformation und Cloud	120
4.3	Überlegungen und Anforderungen	122
4.4	Formen von Cloud-Lösungen	123
4.5	Cloud-Service-Modelle	124
4.6	Kriterienkatalog	126
4.7	Cloud-Governance & Cloud-Compliance	128
4.8	Planungsphasen eines Cloud-Projekts	131
4.9	Providersteuerung	136
4.10	Implementierungsstrahl	136
4.11	Checklisten	137
5.	Zentrale Audit- & Zertifizierungsfunktion	139
5.1	Umsetzung	140
5.2	Chinese Walls	141
5.3	Lessons Learned	141
5.4	Audit-Schulung	141
5.5	Implementierungsstrahl	143
5.6	Checkliste	144
6.	Nachhaltigkeit	144
6.1	Inhalt und Begriff	144
6.2	Umsetzung von Nachhaltigkeit in der IT	144
6.3	Themenfelder und deren Umsetzung	145

Inhaltsverzeichnis

6.4	Implementierungsstrahl	146
6.5	Checkliste	147
7.	Training & Kommunikation	147
7.1	Zweistufiges Konzept	149
7.2	Adressatenkreis	150
7.3	Kommunikation	150
7.4	Implementierungsstrahl	152
7.5	Checkliste	152
8.	Schriftlich fixierte Ordnung	153
8.1	Mindestanforderungen an Dokumentation	155
8.2	Dokumentation von IT-Systemen	155
8.3	Implementierungsstrahl	157
8.4	Checkliste	158
9.	Tooleinsatz	158
9.1	Planung mit GRC-Tool	159
9.2	Kontrolle & Risikoüberwachung	161
9.3	Antrags- und Freigabe-Funktion	161
9.4	Automatisierte Berichterstattung	161
9.5	Archivierung, Ordnung und Hinterlegung	161
9.6	Unterstützung von Audits	162
9.7	MS Sharepoint für gemeinsame Arbeit	162
9.8	Implementierungsstrahl	162
9.9	Checkliste	163
Anhang		164
	Rollen im IT-Governance-Themenumfeld	164
	Mustervorlage sfO	167
	Mustervorlage Kontrolldokumentation	169
	Mustervorlage SLA	170
	Mustervorlage Vertrag IT-Strat. & IT-Gov.	173

Erläuterung und Übersicht

Im Folgenden werden die übergeordneten Ziele der einzelnen Kapitel dargestellt.

Teil I: Organisation	Das Kapitel „Organisation“ behandelt die für die Organisation der IT-Governance erforderlichen Eckpunkte.
Teil II: Kernthemen	Das Kapitel „Kernthemen“ behandelt die durch die IT-Governance zu regelnden Hauptthemen.
Teil III: Schnittstellenthemen	Schnittstellen-Themen im Sinne dieses Buches sind Themen, die bereits im Schwerpunkt übergeordnet in „allgemeinen“ Abteilungen behandelt werden – allerdings für die IT noch weiterer Präzisierung und Detaillierung bedürfen.
Anhang	Der Anhang beinhaltet Musterbeispiele und Vorlagen.

Tab. 1: Kapitelübersicht

Es folgt eine Übersicht über die Unterkapitel.

Teil I Organisation	Teil II Kernthemen	Teil III Schnittstellenthemen
Begriffsdefinition & Verständnis IT-Governance	IT-Risikomanagement	IKS & Kontrollplan
IT-Organisationsmodell, Aufbau und Ablauforganisation	Kapazitätsplanung, Leistungs- und Performance-Management	Qualitätsmanagement
Prozesshaus	Rechtsradar	IT-Auslagerungsmanagement und Cloud
Methodik, Prinzipien und Leitlinien	Informationsmanagement	Zentrale Audit- & Zertifizierungsfunktion
Gremien, Funktionen und Abteilungen	CMDB & IT-Assetmanagement	Nachhaltigkeit
Berichterstattung	Ressourcenplanung	Kommunikation, Business Enablement & Training
	IT-Compliance	Schriftlich fixierte Ordnung
	Data-Governance	Tooleinsatz
	IT-Architektur & Bebauung	
	Strategische Entwicklung der IT	

Tab. 2: Übersicht der Unterkapitel



Coffee Corner - wie alles begann...

In der **Resilient & Erfolgreich AG** bleibt einem offenbar gar nichts erspart. Erst die Umstrukturierung und jetzt auch noch das riesige und nervenaufreibende Projekt „**Captain Future**“ mit dem man einen guten Standard in der IT, der IT-Steuerung sowie den daran angrenzenden Themenbereichen wie Informationssicherheit und dem Informationsrisikomanagement erreichen möchte.

Die neue Abteilung IT-Steuerung soll ausgerechnet mit den unmöglichen Kollegen aus dem IT-Betrieb der konzerneigenen Bank aufgebaut werden. Mr. „Grumpy Cat“ aus der Rechtsabteilung soll dazu den Rechtsrat erteilen. Zu guter Letzt muss man sich auch noch mit der Informationssicherheit bzw. dem Informationsrisikomanagement abstimmen. Wie soll das denn alles funktionieren? Entsprechend hakelig läuft das Projekt an.

Nach einer Woche ruft der Projektleiter alle Beteiligten des Projektes „**Captain Future**“ in die **Coffee Corner**. Für den nächsten Abend sei in einem Restaurant für ein gemeinsames Abendessen reserviert. Bei den ersten Gläsern Wein bei „Alberto“ wird die Stimmung sodann lockerer und in der Karaoke Bar schließlich heiter – als man gemeinsam als die „**Cyber Chiefs**“ den Song „**Modern Way**“ interpretiert.

Am nächsten Tag werden im gemeinsamen Workshop erste Konturen von Teamgeist erkennbar. Seltsamerweise kein Genörgel. Dafür versucht man, konstruktiv die Position des anderen zu verstehen. Ferner kommt man auch darüber überein, die entdeckte gemeinsame Leidenschaft für Musik fortan in die tägliche Arbeit so gut es geht einzuflechten.

It's the only way of getting out of there (Kaiser Chiefs – Modern Way)

Teil I: Organisation

1. Begriffsdefinition & Verständnis

IT-Governance ist die Struktur zur **Steuerung** sowie **Überwachung des Betriebs** und der **Weiterentwicklung der IT-Systeme** einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie.¹ Maßgeblich für die Steuerung durch die IT-Governance sind die Zielsetzungen aus der **IT-Strategie** sowie aus dem **übergeordneten Risikomanagement**.



Coffee Corner

Time stand still (Rush – Time stand still)

Der Startschuss der Geschichte der Informationstechnologie kann bei Konrad Zuse im Jahr 1941 angesetzt werden. Er gilt als Erfinder der ersten voll funktionsfähigen Rechenmaschine, wie wir sie heute kennen. Konrad Zuse prognostizierte im Vertrauen auf seine Vision zutreffend den Bedarf für seine Erfindung. Im Rahmen der Geschichte der IT gab es aber auch eine Reihe beachtlicher unzutreffender Prognosen. Ein Auszug:

- „Ich denke, der Weltmarkt liegt bei vielleicht fünf Computern“ (Thomas Watson 1943, damaliger Chef von IBM)
- „Es gibt keinen Grund, warum irgendjemand einen Computer in seinem Haus wollen würde“ (Ken Olsen, Präsident, Vorsitzende und Gründer von DEC)
- „Internet ist nur ein Hype“ (Bill Gates 1995)

Wären die Fehlprognosen mit ausreichender Strategiewerkarbeit vermeidbar gewesen – und welchen Beitrag hätte eine IT-Governance dazu leisten können?

Die IT-Governance hat als Hauptaufgabe, die **in der IT-Strategie formulierten Ziele** im Tagesgeschäft umzusetzen. Dafür muss sie im Kern sicherstellen, dass IT-Aktivitäten mit den aktuellen und zukünftigen Anforderungen des Business abgestimmt sind. Der Fokus liegt somit auf der ständigen Optimierung und Weiterentwicklung der Organisationsstrukturen, der IT-Prozesse, der Servicequalität und der Effizienz der Serviceerbringung sowie dem Schaffen von Grundlagen für die Steuerung von Risiken. Daneben hat sie insbesondere eine ordnende und orchestrierende Funktion.

¹ Tz.2.1 S.1 Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021 der Bundesanstalt für Finanzdienstleistungen.



Coffee Corner

Said it's up to me, to come up with a strategy (Archie Bell & The Drells - Strategy)

In einer Workshoppause erklärt ein Vorstand der **Resilient & Erfolgreich AG** bei Kaffee und Kuchen, IT-Governance sei für ihn immer noch nicht ganz greifbar. Er habe zwar nun so ungefähr verstanden, dass diese insbesondere Planungs- und Umsetzungsaktivitäten beinhalte. Nach seiner Wahrnehmung werde damit aber nur künstlich ein zusätzlicher Verwaltungsapparat aufgebaut. Dabei habe man doch das Projekt „**Captain Future**“ u.a. gerade deswegen initiiert, um Kosten zu senken.

Nach dem Pausengong startet der Workshop in die 2. Hälfte. Es gibt zunächst größeres Gemurmel. Daraufhin verliert Workshopteilnehmer **Paul Peilung** (Leiter IT-Governance) die Kernziele der IT-Strategie. Am Punkt „Vorhaben zur Konsolidierung der Rechenzentrumslandschaft“ entzündet sich eine hitzige Debatte. Das sei seit Jahren geplant, aber es passiere einfach nichts, erklärt **Stefan Stabil** (Leiter IT-Operations). Dabei hätte die längst geplante Konsolidierung der Rechenzentren bis heute Einsparungen in sechstelliger Größenordnung gebracht.

Mit seiner theatralischen Brillenabsetzgeste bringt der Vorstand seine Erkenntnis zum Ausdruck, dass die Nachhaltung der Umsetzung der Ziele nicht minderes Gewicht hat wie deren Formulierung.

Strategie und ihre Umsetzung sind maßgebliche Faktoren für Erfolg und Misserfolg eines Unternehmens. Der **moderne Wettbewerb** ist **zu hart für dauerhafte Erfolgsgeschichten** von **Glücksgriffen** und **Zufallsprodukten**. So wichtig die strategischen Ziele sind, so entscheidend ist jedoch auch die **richtige Umsetzung**. Dieses Element wurde gerade bei der IT lange vernachlässigt.

1.1 Aufbau- und Ablauforganisation

Die IT-Organisation beinhaltet die Aufbau- und Ablauforganisation in der IT und beschreibt alle wesentlichen Aspekte ihrer Organisation. Die **IT-Aufbauorganisation** beschreibt die **Organisationsstruktur** und insbesondere die Leistungsstruktur des IT-Bereichs. Das IT-Organisationsmodell ist die Herangehensweise zur grundsätzlichen Organisation der IT. In modernen IT-Abteilungen schlagen meist „zwei Herzen“. Zum einen gibt es noch die **klassische IT**, zum anderen kommen meist bereits **agile Modelle oder Hybridformen** beider Organisationsmodelle zum Einsatz.

Die klassische IT ist i. d. R. nach dem Modell „**Plan-Build-Run**“ ausgerichtet und hat klar getrennte Bereiche für die Steuerung, die Entwicklung und den Betrieb. Dieses Organisationsmodell ermöglicht **hohe Betriebssicherheit und Stabilität**.

Die **agile IT** hat den Vorteil **hoher Geschwindigkeit und Anpassungsfähigkeit**. Gerade in hochdynamischen Geschäftsumfeldern kann meist nur ein agiler Ansatz eine geeignete Wettbewerbsposition ermöglichen. Allerdings müssen hierbei Lösungen gefunden werden, wie konzeptionell sinnvoll gearbeitet und planerischen Anforderungen entsprochen werden kann. Planerische Anforderungen an Projekte ergeben sich insbesondere aus dem **Change Management Office** sowie Regulierungsthemen wie Datenschutz bzw. anderweitiger ggf. tiefergreifender Branchenregulierung.



Good to know

Die Sonne scheint in Strömen - doch wo liegt Strömen bloß (Abstürzende Brieftauben – Kein Plan)

„Agil“ wird in der Praxis auch gerne als „ohne Regeln“ interpretiert - und ist möglicherweise deswegen so beliebt.

Richtig umgesetzt, sind bei agiler Vorgehensweise die Aufwände allerdings nicht minder gering als bei „klassischen“ Modellen. Hintergrund dafür ist, dass die Themen gerade nicht so konkret abgesteckt werden können, wie etwa bei einer Wasserfallmethode. Gerade aber, wenn regulatorische Vorgaben eingehalten werden sollen (z. B. Datenschutz) sind agile Vorgehenskonzepte mit entsprechender (nachweislicher) Dokumentation eine erhebliche Herausforderung. Z. B. muss aus datenschutzrechtlicher Sicht für „Sprints“ im Rahmen des Einsatzes von Data Analytics (eigentlich) ein deutlich **umfassenderes Prüfungsprogramm** absolviert werden, weil darin **sämtliche theoretischen Eventualitäten berücksichtigt** werden müssten.



Coffee Corner

Did you say (that) I've got a lot to learn, well don't think I'm trying not to learn (Frank Sinatra – Teach me tonight)

Wanda Wandel (Project Management Office) der **Resilient & Erfolgreich AG** steht mit einem Espresso in der Coffee Corner und erläutert zu den eben in einem Workshop diskutierten Methoden des Projektmanagements ihre Erfahrung.

Im letzten Projekt war es so, dass nach Abschluss einer Projektphase der Projektleiter in einem Jour Fixe erklärte, man wolle fortan agil arbeiten. Die ganze Planungsarbeit „nerve“, sei zeitraubend und man käme im Übrigen viel langsamer zum Ziel. Außerdem sei es nicht mehr zeitgemäß, detailliert und womöglich noch „**per Wasserfall**“ zu planen. Einer der Workstreams blieb infolge der ursprünglichen Planung bei der Wasserfallmethode. Der Workstream erzeugte im Projekt (als einer der wenigen im Programm) zufriedenstellende Arbeitsergebnisse und liefert „in Time & Budget“. Ihr fragt mich, was aus meiner Sicht der Grund für die erfolgreiche Arbeit mit der „altmodischen“ Methode war?

Der erfolgreiche Workstream erarbeitete konzeptionelle Fragen. Diesbezüglich war es deutlich passender, „per Wasserfall“ nach vorne zu arbeiten und erst nach Konsolidierung und abgestimmten Feinkonzepten in die neuen Phasen überzugehen. Der parallel verlaufende Stream hatte ebenfalls gleichgelagerte konzeptionelle Inhalte zum Gegenstand. Allerdings arbeitete dieser Workstream mit agilen Methoden. Das führte jedoch dazu, dass „Sprints“ mit aufwändigen und **nervenauffreibenden Reconciliation-Runden** immer wieder auf Basis neuer Maßgaben aktualisiert werden mussten. Meine Lehren daraus? Die Methoden müssen zum Vorhaben passen.

Die IT-Governance sollte ein Steuerungskonzept sein auf dessen Basis „end-to-end“ durchgesteuert werden kann. Das bedeutet aber nicht, dass sämtliche Details bis in die **letzte Verästelung geregelt** werden müssen.