IT-Governance

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

Wolfgang Gaess

Fachmedien Recht und Wirtschaft I dfv Mediengruppe I Frankfurt am Main

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

www.ruw.de

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 Begleitmangelerscheinungen. 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 gesamtheitlich 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. OpRisk[1]). Themen, die mithin durch die KRITIS-Verordnung, die zunehmenden Zertifizierungserfordernisse wie TISAX[2] oder nach ISO sowie anerkannte Prüfungsstandards wie ISAE[3] (bzw. IDW PS[4]) 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.

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 **Cyberrisiken** sowie den **unterstützenden Ordnungsthemen** aufgrund ihres **hohen Regulierungsgrades bzw. der Regulierungsdichte anderen Industrien voraus** (insbesondere in Form von MaRisk[5] und BAIT[6] 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 Informationstechnik[7], 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

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 Strategiearbeit 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 verliest 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 sechsstelliger 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 **nervenaufreibenden 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.