

Nutzenpotenziale regulatorischer Anforderungen zur Geschäftsoptimierung im Rahmen der digitalen Transformation

Michael Kranawetter, National Security Officer
Microsoft Deutschland GmbH

Neufassung Juni 2017



INHALTSVERZEICHNIS

	ERLÄUTERUNGEN ZUM INHALT	4
1.	PROLOG.....	5
1.1	Vorworte	6
2.	EXECUTIVE SUMMARY – COMPLIANCE ALS NUTZBRINGER FÜR DEN GESCHÄFTSERFOLG	12
3.	DIE DIGITALE TRANSFORMATION UND DIE CLOUD.....	16
3.1	Entwicklungen der digitalen Transformation	16
3.1.1	Technologien, Trends und Ziele.....	16
3.1.2	Digitalisierung von Geschäftsprozessen.....	18
3.1.3	Digitaler und mobiler <i>Workspace</i>	19
3.1.5	Internet der Dinge	19
3.2	Herausforderungen der digitalen Transformation	20
3.2.1	Kooperation durch übergreifende <i>Workflows</i>	20
3.2.2	Mobilität, Flexibilität, Sicherheit	21
3.2.3	Schnelle und automatisierte Kommunikation	22
3.3	Strategische Aspekte der digitalen Transformation	23
3.3.1	Technologische Entwicklungen.....	23
3.3.2	<i>Cloud</i> als Basistechnologie	24
4.	COMPLIANCE UND DIE DIGITALE TRANSFORMATION.....	26
4.1	Compliance – eine Einführung	26
4.1.2	<i>IT Compliance</i> und <i>Corporate Compliance</i> – Grenzen verschwimmen	27
4.1.3	<i>IT Compliance</i> – eine Frage der Sicherheit?	29
4.2	Compliance und Cloud: Risiko oder Chance?	32
4.2.1	<i>Compliance</i> als Strategie für <i>Cloud</i> -Anbieter	32
4.2.2	Wie unterstützt die <i>Cloud</i> die Umsetzung von <i>Compliance</i> ?	34
4.2.3	<i>Compliance as a Service</i> ? Leichter als gedacht!	36
4.3	Resümee: Compliance wird digitaler und standardisierter	37
5.	COMPLIANCE UND GESCHÄFTSERFOLG VERBINDEN – EIN MODELL	40
5.1	Compliance als strategischer Ansatz	40
5.1.1	<i>Compliance</i> aus <i>Governance</i> -Sicht	40
5.1.2	<i>GRC</i> – <i>Governance</i> , <i>Risk Management</i> und <i>Compliance</i>	41
5.2	Mit Compliance zum Geschäftserfolg	42
5.2.1	Nutzenpotenziale resultieren aus gemeinsamen Zielen	42
5.2.2	Kernbereiche regulatorischer und geschäftlicher Anforderungen.....	45

6.	ANWENDUNG DES COMPLIANCE-MODELLS	54
6.1	Vom Verständnis- zum Anwendungsmodell	54
6.1.1	Verfeinerung des Modells	54
6.1.2	Analyse als Basis für unternehmerisches Handeln	55
6.2	Handlungsfelder zur Verbesserung des Geschäftserfolges	56
6.2.1	Informationssicherheit und -schutz	56
6.2.2	Umgang mit IT-Compliance-Risiken	57
6.2.3	Informations- und Kommunikationsmanagement	58
6.2.4	Bilanztheorie, Prüfungswesen und Organisation	58
6.2.5	Informations- und Transparenzpflicht	59
6.2.6	Globalisierung und Transformation	59
6.3	Compliance-Prozesse beurteilen und verbessern	60
6.3.1	Ansatz 1: Nutzung eines qualitativen Reifegradmodells	60
6.3.2	Ansatz 2: KPMG Self-Assessment	64
7.	BEITRAG DER CLOUD ZU COMPLIANCE UND GESCHÄFTSERFOLG	68
7.1	Cloud-Service-Modelle im Vergleich	68
7.1.1	Übertragung von Zuständigkeiten	68
7.1.2	Steuerung des Anbieter-Kunden-Verhältnisses	70
7.2	Anwendungsbeispiele	70
7.2.1	Compliance, Informationssicherheit und -schutz	70
7.2.2	Cloud-Dienste für mehr Dynamik und Flexibilität	72
7.3	Die Cloud als Win-win-Strategie	74
8.	EPILOG	75
9.	AUTOREN	76
10.	GLOSSAR	77
11.	ANALYSTENFAZITS – ISG GROUP	85
11.1	Über ISG	85
11.2	Analystenfazits	85
	ABBILDUNGSVERZEICHNIS	87
	COPYRIGHT	87

ERLÄUTERUNGEN ZUM INHALT

Kapitel 2: *Executive Summary* – *Compliance* als Nutzbringer für den Geschäftserfolg

Dieses Kapitel enthält ein *Executive Summary*, das die wesentlichen Überlegungen dieses Handbuchs zusammenfasst.

Kapitel 3: Die digitale Transformation und die *Cloud*

Dieses Kapitel untersucht die Auswirkungen der digitalen Transformation auf Geschäftsprozesse und arbeitet heraus, warum *Cloud*-Anwendungen eine Basistechnologie für diese Entwicklung darstellen.

Kapitel 4: *Compliance* als Chance der digitalen Transformation

Dieses Kapitel verdeutlicht, dass die Erfüllung von *Compliance*-Anforderungen nicht nur eine lästige Pflicht ist, sondern einen geschäftlichen Nutzen mit sich bringt. *Cloud*-Lösungen unterstützen die Umsetzung von *Compliance*-Anforderungen und tragen gleichzeitig zum geschäftlichen Nutzen bei.

Kapitel 5: Entwicklung des *Compliance*-Modells

Dieses Kapitel stellt ein *Compliance*-Modell vor, das aus regulatorischen und geschäftlichen Zielen sechs Kernbereiche ableitet. Mit der Bearbeitung dieser Kernbereiche lässt sich die Grundidee dieses Handbuchs umsetzen: die Erfüllung von *Compliance* bei hohem Nutzwert für das Geschäft.

Use Cases

Anhand von Beispielen wird untersucht, welchen Beitrag die verschiedenen *Cloud*-Modelle für die Umsetzung von *Compliance*-Anforderungen und gleichzeitig für den Geschäftserfolg leisten.

Kapitel 6: Anwendung des *Compliance*-Modells

Dieses Kapitel verfeinert das *Compliance*-Modell, indem aus den sechs Kernbereichen Handlungsfelder abgeleitet werden. Das fertige Modell lässt sich in zwei unterschiedlichen Szenarien einsetzen, die beide den aktuellen Stand der *Compliance*-Prozesse messen und Ausgangspunkt für Verbesserungen sind.

Kapitel 7: Beitrag der *Cloud* zu *Compliance* und Geschäftserfolg

In diesem Kapitel wird insbesondere der Mehrwert zur Erfüllung von *Compliance*-Anforderungen bei der Nutzung von *Cloud*-Technologie erörtert.

Analystenfazit:

Die digitale Transformation stellt neue Herausforderungen an die Erfüllung von *Compliance*-Anforderungen. Diese waren Anlass für die Weiterentwicklung des *Compliance*-Modells.

1. PROLOG

Compliance ist und bleibt ein Thema, dem sich keine Organisation, kein Unternehmen und auch keine Behörde verschließen kann. Gerade heute ist zudem das Motto der **Digitalisierung** und der damit verbundenen Notwendigkeit einer **Transformation** in die digitale Welt in aller Munde. Die Veränderung des täglichen Lebens durch Technologie schreitet unaufhaltsam fort, auch und gerade außerhalb der klassischen Einsatzbereiche der IT.



Mit der digitalen Transformation verbinden sich viele Hoffnungen:

- Neue und flexible Geschäftsmodelle lassen sich entwickeln.
- Prozesse lassen sich neu abbilden und komplett automatisieren.
- Informationen lassen sich genauer und optimiert in Entscheidungen einarbeiten.
- Kunden können besser eingebunden und betreut werden.
- Kostenstrukturen lassen sich verbessern.

Mit der digitalen Transformation gehen aber auch signifikante Veränderungen in der Arbeitswelt wie auch im Privaten und somit den Gewohnheiten der Menschen einher.

Neben diesen ganz offensichtlichen Auswirkungen dieses **Paradigmenwechsels** sind aber noch andere Aspekte von entscheidender Bedeutung. Ganz vorne stehen dabei die Herausforderungen, die sich durch die **Dynamik**, die **Flexibilität** und die **Offenheit** der Digitalisierung ergeben, sowie die Fragestellung, wie sich unter diesen Gesichtspunkten neue und bestehende **Compliance-Anforderungen** in der Regel basierend auf **Schutz-, Verfügbarkeit-, Nachvollziehbarkeit-, Transparenz- und Sorgfaltspflichten** umsetzen lassen.

Im Jahre 2009 stellte Microsoft zusammen mit der damaligen Experton Group (jetzt ISG Germany) ein **Compliance-Handbuch** vor, in dem ein **Reifegradmodell** zur Bestimmung des eigenen Status in Bezug auf **Compliance** entwickelt wurde (NUTZENPOTENZIALE REGULATORISCHER ANFORDERUNGEN ZUR GESCHÄFTSOPTIMIERUNG). Dieses Modell ist in seinen Grundzügen heute noch gültig. Allerdings war zu diesem Zeitpunkt die fortschreitende Digitalisierung zwar absehbar, aber nicht in der Dimension und Wucht, wie sie heute auf **Wirtschaft, Gesellschaft und Staat** wirkt. Deshalb war das Thema Digitalisierung inklusive **Cloud Computing** kein Schwerpunkt des Modells.

In dieser Neuauflage des Handbuchs werden die Erfahrungen der letzten Jahre mit dem Modell sowie die neuen Aspekte der digitalen Transformation eingebracht. Parallel dazu wurde das Modell von der Wirtschaftsprüfungsgesellschaft KPMG weiterentwickelt und um aktuelle Fragestellungen ergänzt. Der Kern des Modells, die Formulierung gemeinsamer Ziele für **regulatorische** und **geschäftliche Anforderungen**, ist gleich geblieben und wurde lediglich auf einen aktuellen Stand gebracht.

Wir denken, dass mit dieser Aktualisierung der Wert dieses Handbuchs erhalten bleibt und es ebenso gerne in die Hand genommen wird wie sein Vorgänger. Die Ideen und Modelle des Handbuchs können dazu beitragen, die **Herausforderungen** der digitalen Transformation und die **Erfordernisse** der **Compliance** in Einklang zu bringen, zum Nutzen von Unternehmen, Behörden, aber vor allem der Anwender, die einen immer größeren Teil ihres Alltags in digitale Welten verlagern.

Michael Kranawetter

Head of Information Security, National Security Officer Germany
Microsoft Deutschland GmbH

1.1 Vorworte



Alexander Gietl ist seit 2005 in der Münchner Niederlassung der KPMG AG beschäftigt. Als Director im Bereich *IT Compliance* unterstützt er zahlreiche globale und internationale Unternehmen bei der Ausgestaltung der regulatorischen Vorgaben für Organisation, Steuerung und Kontrolle der IT sowie bei der angemessenen und ordnungsgemäßen Ausrichtung von IT-gestützten Prozessen, inklusive Bescheinigung und Zertifizierung von IT-Produkten und IT-Dienstleistungen.

Microsoft und KPMG sind Partner im Rahmen einer strategischen Allianz. Hierbei liegt ein Fokus auf der Zusammenarbeit zur Entwicklung und Lieferung innovativer sowie ordnungsgemäßer Lösungen in den Bereichen *Data & Analytics*, *Cloud Compliance* und Transformation sowie Unternehmenssoftware (ERP & CRM).

Die Zahl der Regelwerke und Vorgaben – das heißt interne und externe Regelwerke sowie gesetzliche Vorgaben – steigt kontinuierlich an. Diese betreffen meist auch die IT, und somit ist die **Einhaltung dieser Vorgaben** zu einem **Erfolgsfaktor** geworden, um die digitalen Herausforderungen zu meistern – ein Erfolgsfaktor, der abteilungsübergreifend alle Unternehmensprozesse erfasst. Denn mit jeder neuen Technologie, der globalen Digitalisierung sowie dem stetigen Ruf nach vertrauenswürdigen Finanzzahlen wächst der externe und interne Regelungsbedarf und somit die Bedeutung der *IT Compliance*.

Unter anderem ergeben sich hierzu für die Unternehmen folgende Grundsatzfragestellungen:

- Sind die *IT-Compliance*-Regelungen in meinem Unternehmen transparent erfassbar?
- Sind Regelungen zur *Compliance* der IT-Funktion sowie auch zur IT-gestützten *Corporate Compliance* gleichermaßen berücksichtigt?
- Gibt es in meinem Unternehmen Prozesse, die die Einhaltung der *IT-Compliance*-Regelungen kontinuierlich überprüfen und sicherstellen, dass diese nachweislich erfüllt werden?

Doch wo soll man als Unternehmen bzw. als Verantwortlicher für die *IT Compliance* Prioritäten setzen bzw. welche Wesentlichkeiten ergeben sich für mein Unternehmen? Wo soll ich starten? Und welchen Zustand der *IT Compliance* will ich erreichen?

Auch die Frage der **Risikoeinschätzung** zur *IT Compliance* muss individuell für jedes Unternehmen beantwortet werden, um somit ein **optimales Kosten-Nutzen-Verhältnis** zu gewährleisten. Denn der Grundsatz der (*IT*) *Compliance* muss natürlich auch immer dem Aspekt der **Wirtschaftlichkeit** genügen.

Die Digitalisierung in den Unternehmen und in den einzelnen Geschäftsprozessen erfordert somit einen umfassenden und zielgerichteten Ansatz, um den Status der *IT Compliance* einschätzen zu können und unternehmensspezifische Handlungsfelder zu abbilden. Viele regulatorische und geschäftliche Anforderungen verfolgen dabei gemeinsame Ziele: **Schutz** und **Verfügbarkeit** von Informationen, die **Nachvollziehbarkeit** von Prozessen und der Informationsverarbeitung, **Transparenz** gegenüber Dritten, die Erfüllung von **Sorgfaltspflichten** und, im Hinblick auf die digitale Transformation, die Unterstützung der **Dynamik** moderner Geschäftsprozesse und Entwicklungen.

Es gibt vielfältige Ansätze und Bewertungsschemata, um den **Reifegrad** der *IT Compliance* zu messen. Unternehmen sollten hierbei immer auch auf die möglicherweise bereits im Unternehmen bestehenden Grundsätze zu Bewertungsskalen zurückgreifen bzw. diese abstimmen. Es ist allerdings angebracht, mittels eines ganzheitlichen Bewertungsschemas abzufragen bzw. zu analysieren, ob alle relevanten *Compliance*-Anforderungen beachtet wurden und wie gut die Prozesse sind, welche die jeweiligen Handlungsfelder bearbeiten. So sollte ein **Gesamtbild** der *Compliance* unter Betrachtung aller relevanten Prozesse auf Konzern- und/oder Gruppenebene entstehen.

Im vorliegenden Dokument werden im weiteren Verlauf anschaulich Grundsätze und Möglichkeiten zur Einschätzung sowie der **ganzheitlichen Bewertung** der *IT Compliance* aufgezeigt, welche eine pragmatische und umfassende Standortbestimmung bzw. Positionsbestimmung unterstützen sollen.

Alexander Gietl

Director im Bereich IT Compliance, KPMG AG

Rechtsanwalt Prof. Dr. Josef Scherer ist seit 1996 Professor für Unternehmensrecht (*Compliance*), insbesondere Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der Technischen Hochschule Deggendorf. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und als Richter am Landgericht in einer Zivilkammer.

Neben seiner Tätigkeit als Seniorpartner der Kanzlei Prof. Dr. Scherer, Dr. Rieger & Partner erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren. Von 2001 bis 2015 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer fungiert in diversen Unternehmen als *Compliance*-Ombudsmann sowie externer Compliance-Beauftragter und ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders ARD-alpha.

In Kooperation mit dem TÜV konzipierte er als Studiengangsleiter und Referent den akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und *Compliance-management* an der Technischen Hochschule Deggendorf und ist als externer Gutachter bei der (System-)Akkreditierung von Weiterbildungsstudiengängen tätig.

Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für *Governance, Management, Risk- und Compliancemanagement* der Technischen Hochschule Deggendorf als Kompetenzzentrum.

Außerdem ist er seit 2015 Mitglied des Beirates des Frankfurter Instituts für Risikomanagement und Regulierung (FIRM, www.firm.fm) und seit 2016 Mitglied des DIN-Normenausschusses Dienstleistungen (Arbeitsausschuss Personalmanagement NA 159-01-19AA) zur Erarbeitung von ISO/DIN-Standards im Personalmanagement.

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Managerhaftung, *Governance*-, Risiko- und *Compliancemanagement* (GRC) sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht.

Zahlreiche Publikationen auf den Gebieten Managerrisiko, *Governance*-, Risiko-, Chancen- und *Compliancemanagement*, Vertragsmanagement, Arbeitsrecht und Personalmanagement, Insolvenzrecht und Sanierung, Gläubigermanagement, Produkthaftungsrecht.



Digitalisierung, Industrie 4.0 und Prozess-/Workflow-Management

1. Was haben *Compliance*-Berufsbilder gemeinsam?

Meine ehemaligen Berufe als Staatsanwalt und Richter und meine jetzigen beruflichen Tätigkeiten als Rechtsanwalt in Wirtschafts-(Straf-)Sachen, *Compliance*-Ombudsmann, externer *Compliance* Officer oder Berater im Bereich *Governance, Risk und Compliance* (GRC) haben mehrere gemeinsame Nenner: Alle Funktionen kümmern sich prophylaktisch um pflichtgemäßes Verhalten von Unternehmen, Managern und Mitarbeitern oder reaktiv um

Compliance-Verstöße. Daraus erwächst auch das gemeinsame Bedürfnis nach Diskretion, Datenschutz, Schutz von Informationen also schlichtweg: *Compliance*. In den letzten Jahren wurde von mir aufgrund der zunehmenden Datenflut und Digitalisierung sowie moderner Kommunikationstechniken auch in diesen sehr sensiblen Themenbereichen vermehrt auf *Cloud*-Lösungen gesetzt, um sowohl die Datenmengen steuern als auch die erforderliche Vertraulichkeit gewährleisten zu können.

2. Unternehmen, Manager und Mitarbeiter stoßen auf neue Herausforderungen bei ihrer täglichen Arbeit

Häufig wird der Unternehmensalltag noch durch E-Mails, Excel-Tabellen und mit MS-Office bestritten. Die Prozesse sind oft nicht dokumentiert oder nicht aktuell beziehungsweise nicht nachvollziehbar. Bei Prozessanpassungen müssen teure IT-Spezialisten erst mal die Zeit finden, um die Unternehmen zu unterstützen. E-Mails werden nach Gießkannenprinzip an alle verteilt, sodass jeder in einer E-Mail-Flut versinkt. Sofern Prozesse existieren, sind diese nicht ausreichend mit *Governance*-, *Risk*- oder *Compliance*-Komponenten angereichert.

Ideal wäre es, wenn die Abteilungen im Unternehmen auch ohne teure IT-Spezialisten ihre Prozesse jederzeit selbst aktualisieren könnten. Die Prozesse würden nicht nur dokumentiert, sondern so ausgestaltet, dass – ähnlich wie bei einer Bestellung bei Amazon – die Mitarbeiter geführt durch einen *Human-Workflow* – das Richtige richtig machen müssten. E-Mails würden nur an die tatsächlich zuständigen Adressaten verteilt, und alle Informationen, auch *Compliance*-Regelungen in Richtlinien, würden bei den jeweiligen Prozessschritten bereitgestellt. Automatisch würde auch die Dokumentation und Auswertung der Erfüllung von *Compliance*-Anforderungen oder auch von Prozessdurchlaufzeiten erfolgen. Mit *Workflow*-Management würde der Mensch und Mitarbeiter durch den Prozess geführt und damit zur Zeit- und Systemtreue angehalten.

Mit anderen Worten: Der Mensch und Mitarbeiter, der gerade wegen menschlicher Schwächen auch fehleranfällig ist, würde bei standardisierten Abläufen Fehler nur noch machen können, wenn er bewusst die Prozessvorgaben technisch überwindet und auch Kontrollen in arglistiger Weise ausschaltet.

Die als *Workflows* abgebildeten Prozessabläufe könnten mit allen sonstigen Systemen und Programmen der bereits vorhandenen IT-Landschaft verbunden werden, wie zum Beispiel SAP, Warenwirtschaftssystemen oder Dokumentenmanagementsystemen. Jeder Prozessbeteiligte wüsste, was er wann und wie und wo zu tun hat.

Auch die sogenannten „Überwachungsfunktionen“¹ (*lines of defense*) wüssten neben den Prozessbeteiligten stets, wo der Prozess gerade läuft oder eben auch sich verzögert. So wäre eine Information in Echtzeit möglich und ersparte zahlreiche Nachforschungen, Telefonate oder Meetings. Gerade die „*Compliance*“ würde durch eine stets aktuelle Einbindung von Komponenten zur Erfüllung der Anforderungen aus Gesetzen, Rechtsprechung, internen verbindlichen Regeln oder Richtlinien (wie zum Beispiel Zuwendungs- oder Datenschutzrichtlinien) sowie dem anerkannten Stand von Wissenschaft und Praxis und unter Umständen auch Industriestandards (wie ISO oder COSO – Committee of Sponsoring Organizations of the Treadway Commission etc.) sichergestellt.

Wenn die Aufgaben nicht ordnungsgemäß erfüllt werden, gäbe es keine Krisentelefonate oder Anfälle von Vorgesetzten mehr, sondern eine automatisierte, effektive und effiziente Eskalation zur Behebung der Schwachstelle.

Prozessoptimierungen und Anpassungen würden nicht mehr nach Bauchgefühl, sondern auf der Basis von echten und aktuellen Prozesskennzahlen höchst effizient und effektiv durchgeführt. Über eine der Realität entsprechende Prozesskostenrechnung könnte sowohl der Input

¹ Vgl. Scherer, „Die Welt(en) der Überwacher“, FIRM Jahrbuch 2017, S. 79-81.

des jeweiligen Prozessschrittes als auch der Output in Zahlungsströmen dargestellt werden. Das wäre die Basis für eine Wertbeitragsberechnung nach gelebten Prozessen.²

Das alles ist längst Realität und „Anerkannter Stand von Wissenschaft und Praxis“ bei *Good-practice*-Unternehmen!

Unternehmen bzw. ihre Organe (Aufsichtsrat, Vorstand/Geschäftsführer, Gesellschafter) sind, falls sie selbst nicht pflichtwidrig und haftungsauslösend agieren möchten (§§ 93, 107 AktG, 43 GmbHG, 347 HGB), gehalten, sich an diesen „Anerkannten Stand von Wissenschaft und Praxis“ zu halten.³

Deshalb sollten sie ihre Prozesse dokumentieren, mit Komponenten aus *Governance*, *Risk* und *Compliance* angemessen anreichern und digitalisieren. Sodann jedoch ergeben sich neue Anforderungen: kontinuierliche Gewährleistung der erforderlichen Aktualisierung der enorm gewachsenen Datenmengen, deren Verfügbarkeit und Sicherheit (Datensicherheit, Schutz vor *Cybercrime* und vieles mehr). Da sie dies selbst in der Regel nicht mehr sicherstellen können, sind sie mittelbar gezwungen, auf entsprechend spezialisierte Leistungsanbieter zu delegieren: z. B. auf Anbieter von *Cloud*-Lösungen.

3. Wieso müssen *Cloud*-Anbieter eine besondere Affinität zu *Compliance* haben?

Aufgrund des Verwaltens sensibler Daten in vielfältiger Natur müssen *Cloud*-Anbieter selbst absolut *compliant* sein. Unter anderem auch gerade, weil sie als externe Dienstleister der strengen Kontrolle und Überwachung ihrer Auftraggeber unterliegen: Dies ist ein Ausfluss der „rechtssicheren Delegation“: Der Unternehmer kann nur rechtssicher seiner Organisationsverantwortung entsprechen, wenn er bei Delegation die Externen auch unter *Compliance*-Aspekten sorgfältig auswählt, sie instruiert und kontrolliert. Im Bereich des *Supplier Screening* helfen dem Delegierenden entsprechende Zertifizierungen – auch zur 4.0-Fähigkeit – des externen (IT-)Dienstleisters als Nachweise.⁴

Ein weiterer Punkt, der die besondere Affinität von *Cloud*-Anbietern zu *Compliance* begründet, besteht darin, dass – wie oben dargestellt – die diversen unternehmerischen Aktivitäten vermehrt als *Workflows* digitalisiert und in *Clouds* vorgehalten werden. *Cloud*-Anbieter in der Rolle als Unterstützer der Unternehmen im Bereich der Prozessdigitalisierung sollten auch Hilfestellung bei der Anreicherung der Unternehmensprozesse mit Komponenten aus *Governance*, *Risk* und *Compliance* und Umwandlung in *Workflows* geben können, damit die von ihnen vorgehaltenen und verwalteten digitalisierten Prozesse auch den Anforderungen diverser Regulierungen und „*interested parties*“ entsprechen. Dadurch entstünde für den *Cloud*-Anbieter ein Alleinstellungsmerkmal in der Zusammenarbeit mit den Kunden und für Kunde und Anbieter eine Win-win-Situation.

„Es gibt noch viel zu tun ... fangt schon mal an!“⁵

Prof. Dr. Josef Scherer

Professor für Unternehmensrecht (*Compliance*)
an der Technischen Hochschule Deggendorf

² Vgl. Ludacka, Workflow-Management, in: Scherer/Fruth, Integriertes Compliance-Managementsystem mit GRC, 2. Auflage, 2017, Punkt 1.2.5.

³ Vgl. Scherer/Fruth, Geschäftsführer-Compliance, 2009; Scherer/Fruth, Governance-Management, Band 1, 2014, und Band 2, 2015; Scherer/Fruth, Der Einfluss von Standards, Techniklauseln und des „Anerkannten Standes von Wissenschaft und Praxis“ auf Organhaftung und Corporate Governance, Corporate Compliance Zeitschrift, 2015, S. 9-17.

⁴ Vgl. Scherer, Business Partner Screening – Überwachungspflichten bei Delegation von Aufgaben auf Externe, in: Scherer/Fruth, Integriertes Personal-Managementsystem mit GRC, 2017, Anlage 3.

⁵ Vgl. Scherer/Fruth, Integriertes „GRC-Kombi-Managementsystem on demand“, 2017, und Scherer, Thesenpapier zu digitaler Transformation (Digitalisierung), Industrie 4.0, „digital workflow management“ und integriertem Managementsystem unter dem Aspekt von Governance, Risk und Compliance (GRC), 2017.



Prof. Dr. Michael Amberg studierte Informatik in Aachen und Erlangen. 1993 promovierte er in Bamberg über objektorientierte Softwareentwicklungen; 1999 folgte die Habilitation über Methoden, Vorgehen und Werkzeuge für prozessorientierte Informationssysteme. Von 1999 bis 2001 war er Professor für Wirtschaftsinformatik an der RWTH Aachen.

Seit 2001 ist Michael Amberg Inhaber des Lehrstuhls für Wirtschaftsinformatik, insbesondere IT-Management, an der FAU Erlangen-Nürnberg. Von 2007 bis 2012 war er in wechselnder Funktion als Sprecher des Fachbereichs Wirtschaftswissenschaften und als Prodekan bzw. Dekan der Rechts- und Wirtschaftswissenschaftlichen Fakultät tätig. Michael Amberg ist im Vorstand des Alumnivereins der FAU Erlangen-Nürnberg und seit 2010 Vorstand des Dr. Theo und Friedl Schöller Forschungszentrums für Wirtschaft und Gesellschaft.

Die Fortschritte bei der Informationsverarbeitung und bei den Informationstechnologien haben einen neuen Höhepunkt erreicht. Wer hätte noch vor wenigen Jahren erahnt, dass wir schon jetzt in der Lage sein werden, auch mit größtmöglichen Datenmengen effizient umzugehen und diese umfassend auszuwerten. Zudem steht für die datenintensive Informationsverarbeitung eine bisher unerreichte Qualität von *Cloud*-Dienstleistungen und *Cloud*-Dienstleistern zur Verfügung.

Unternehmen fragen sich heutzutage nicht, ob sich das umfassende Sammeln von Daten lohnt und man aus den großen Datenbeständen wertvolles Wissen generieren kann. Vielmehr geht es darum, schneller, besser, umfassender und effektiver als die Wettbewerber zu sein.

Dabei werden sicherlich Grenzen der Informationsverarbeitung neu ausgelotet. Und wenn man nicht aufpasst, ggf. auch regulatorische Grenzen überschritten. Dies stellt die *Compliance* vor völlig neue Herausforderungen. Einerseits möchte man die Umsetzung der unternehmerischen Potenziale nicht behindern, andererseits aber auch kein Fehlverhalten ermöglichen, das sich ggf. kurz- oder langfristig negativ auf den Unternehmenserfolg auswirken kann, wie jüngste Skandale eindrucksvoll belegen.

Vor welchen großen Herausforderungen steht die unternehmerische Informationsverarbeitung aktuell? Wie genau wirken sich diese Herausforderungen auf die Anforderungen an *Compliance* aus? Was sind die derzeit wichtigsten Handlungsfelder der *IT Compliance*? Und wie sieht eine umfassende methodische Hilfestellung zur Positionsbestimmung und Weiterentwicklung der *IT Compliance* aus? Darauf gibt das vorliegende Handbuch eine fundierte Antwort.

Prof. Dr. Michael Amberg

Professor für Wirtschaftsinformatik
an der FAU Erlangen-Nürnberg

KAPITEL 2

11

EXECUTIVE SUMMARY –
COMPLIANCE ALS NUTZBRINGER
FÜR DEN GESCHÄFTSERFOLG

2. EXECUTIVE SUMMARY – COMPLIANCE ALS NUTZBRINGER FÜR DEN GESCHÄFTSERFOLG

Der Handlungsbedarf bei der Umsetzung von *Compliance*-Anforderungen wächst unaufhaltsam, nicht zuletzt getrieben durch die fortschreitende Verlagerung von Geschäftsprozessen und *Workflows* in die digitale Welt. Die digitale Transformation und der damit einhergehende verstärkte Einsatz von *Cloud*-Lösungen hat nicht nur Auswirkungen auf Geschäftsprozesse, die Einbindung von Mitarbeitern oder das Verhältnis zu Kunden, sondern bringt eine Dynamik ins Spiel, die die Erfüllung von *Compliance*-Anforderungen vor neue Herausforderungen stellt.

Dabei ist die Erfüllung von *Compliance*-Anforderungen längst mehr als nur eine lästige Pflicht. Die im Zusammenhang mit *Compliance* umgesetzten Maßnahmen haben auch einen positiven Effekt für den eigenen **Geschäftserfolg**. Die Frage stellt sich:

Wenn Regularien ohnehin umgesetzt werden müssen, wie kann aus dieser Umsetzung ein maximaler Nutzen für das eigene Geschäft gezogen werden?

Dabei stehen regulatorische und geschäftliche Anforderungen nicht im Widerspruch zueinander. Im Gegenteil: Beide lassen sich auf gemeinsame Zielsetzungen und Intentionen zurückführen. Unternehmen können regulatorische Vorgaben als Ausgangspunkt nutzen, um Synergieeffekte zwischen den vorgegebenen Pflichten und den eigenen Zielsetzungen zu realisieren.

Welche Schritte müssen unternommen werden, um dieses Ziel zu erzielen?

Zur Vereinfachung haben wir ein *Compliance*-Modell entwickelt, das die Komplexität des Themas stark reduziert und zu einem besseren Verständnis beiträgt. Dabei verfolgen regulatorische und geschäftliche Anforderungen – mit Blick auf Informationen – sechs gemeinsame Ziele: **Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz, Sorgfalt** und **Dynamik**. Diese Ziele basieren auf gesetzlichen und regulatorischen Grundwerten und liegen in der einen oder anderen Form den meisten Regelungen zugrunde. Lediglich die Ausprägung unterscheidet sich von Land zu Land und von Regelung zu Regelung.

Diese geschäftlichen und regulatorischen Vorgaben und Ziele können in der Regel über Prozesse aus den folgenden sechs Kernbereichen erfüllt werden:

- Informationssicherheit und -schutz
- Umgang mit Risiken
- Informations- und Kommunikationsmanagement
- Bilanztheorie, Prüfungswesen und Organisation
- Transparenz- und Informationspflicht
- Globalisierung und Transformation

Das sind die gemeinsamen Themenfelder, die sich aus den gesetzlichen und betriebswirtschaftlichen Anforderungen herauskristallisieren.

Ein Unternehmen, das in diesen Kernbereichen gut aufgestellt ist, kann künftige *Compliance*-Anforderungen besser umsetzen. Wer sich also auf die sechs genannten Bereiche konzentriert, nutzt *Compliance* auch als Treiber für eine dynamische IT-Infrastruktur. Außerdem werden für geschäftliche Anforderungen zusätzlich Nutzenpotenziale geschöpft, darunter die Kalkulierbarkeit und Reduzierung von Geschäfts- und IT-Risiken, die Vermeidung von Betrugsfällen, mehr Effizienz und Transparenz durch die Automatisierung und Optimierung von Prozessen, die erhöhte Reputation des Unternehmens insgesamt und letztlich auch die Optimierung von Investitionen in Schutzmaßnahmen.

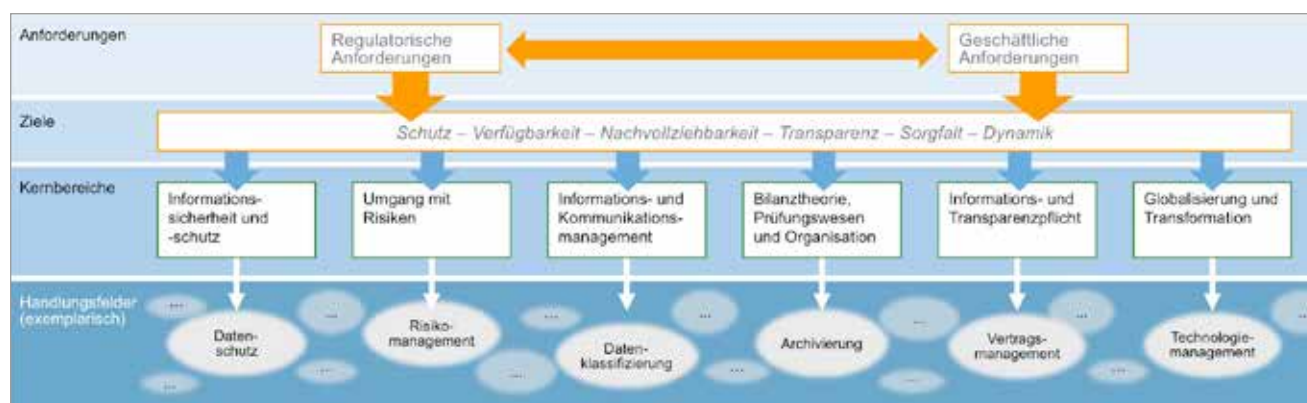


Abbildung 1: Zusammenfassung des *Compliance*-Modells

Die Auseinandersetzung mit diesem Thema hilft, dein Verständnis für die Problematik zu entwickeln. Jedoch müssen auch konkrete Schritte für die Umsetzung unternommen werden, die abhängig von der bestehenden Ist-Situation sind.

Die Frage stellt sich, wie ein Unternehmen überhaupt seinen aktuellen *Compliance*-Zustand und das angestrebte Ziel erkennen kann.

Durch die Analyse des Ist-Status eines Unternehmens bezüglich der Umsetzung der Ziele und Kernbereiche des *Compliance*-Modells können Handlungsfelder identifiziert werden, über die sowohl *Compliance* umgesetzt als auch der eigene **Geschäftserfolg** vergrößert werden. Ein Unternehmen, das sich umfassend und bereichsübergreifend mit der Analyse der eigenen Prozesslandschaft auseinandersetzt, erhält auf diese Weise einen Überblick über all jene Bereiche, in denen die Erreichung regulatorischer und geschäftlicher Ziele verbessert werden kann.

Das beschriebene *Compliance*-Modell holt Ihr Unternehmen dort ab, wo es momentan steht.

Das Modell zeigt einfache Schritte, um sich dem Thema *Compliance* anzunähern und eine gemeinsame Kommunikationsebene zu schaffen. Dabei ist klar, dass ein vereinfachtes Modell keinen Anspruch auf Vollständigkeit erhebt. Jedoch wird das Modell helfen, eine Grundlage für das Verständnis von *Compliance* und deren Beitrag zur Geschäftsoptimierung zu schaffen. Naturgemäß muss bei einer vertieften Betrachtung auf die jeweilige individuelle Situation des Unternehmens eingegangen werden, auch wenn sich die grundlegenden Strukturen immer wieder gleichen.

Das Modell kann auf zwei Arten eingesetzt werden:

- Über die qualitative Einordnung von Prozessen, mit denen bestimmte Handlungsfelder in den sechs Kernbereichen umgesetzt werden, ist die Bestimmung des Reifegrades der eigenen *Compliance*-Anstrengungen möglich. Dies erleichtert es dem Unternehmen, **den eigenen Standort zu bestimmen** und seine aktuelle Risikosituation darzustellen. Es wird transparent, welcher Status vorliegt und wie ein **übergreifendes Zusammenspiel** der Beteiligten zur Verbesserung beitragen kann.
- Der andere Ansatz, Defizite in den zur Erreichung von *Compliance* wesentlichen Handlungsfeldern zu identifizieren, ist das *KPMG Self-Assessment*. Mittels eines Online-Fragebogens wird bei diesem *Assessment* systematisch abgefragt, ob alle relevanten *Compliance*-Anforderungen beachtet wurden. So entsteht ein Gesamtbild der *Compliance* unter Betrachtung aller relevanten Prozesse. Zudem wird eine **detaillierte Ergebnisanalyse** durchgeführt, aus der sich **Handlungsfelder** und letztlich **konkrete Maßnahmen** zur Verbesserung bestimmter *Compliance*-Prozesse herleiten lassen.

Beide Einsatzszenarien liefern wertvolle Erkenntnisse, wo es bei der eigenen *Compliance* noch hakt und wo Verbesserungspotenziale liegen. Damit können Unternehmen und Behörden die neuen Herausforderungen, die sich durch die digitale Transformation und den Einsatz von *Cloud*-Lösungen stellen, systematisch und nutzbringend bewältigen.

Ein ergänzendes Kapitel beschäftigt sich mit der Rolle der *Cloud* bei der Erfüllung von *Compliance*-Anforderungen. An zwei Beispielen aus dem Katalog der Handlungsfelder des Modells wird deutlich, welchen Beitrag die verschiedenen *Cloud*-Modelle hier leisten.

Analystenfazit:

Mit dem *Compliance*-Modell kann der aktuelle Status der eigenen *Compliance* einfach und anschaulich ermittelt werden. Zudem werden Potenziale für Verbesserungen sichtbar.

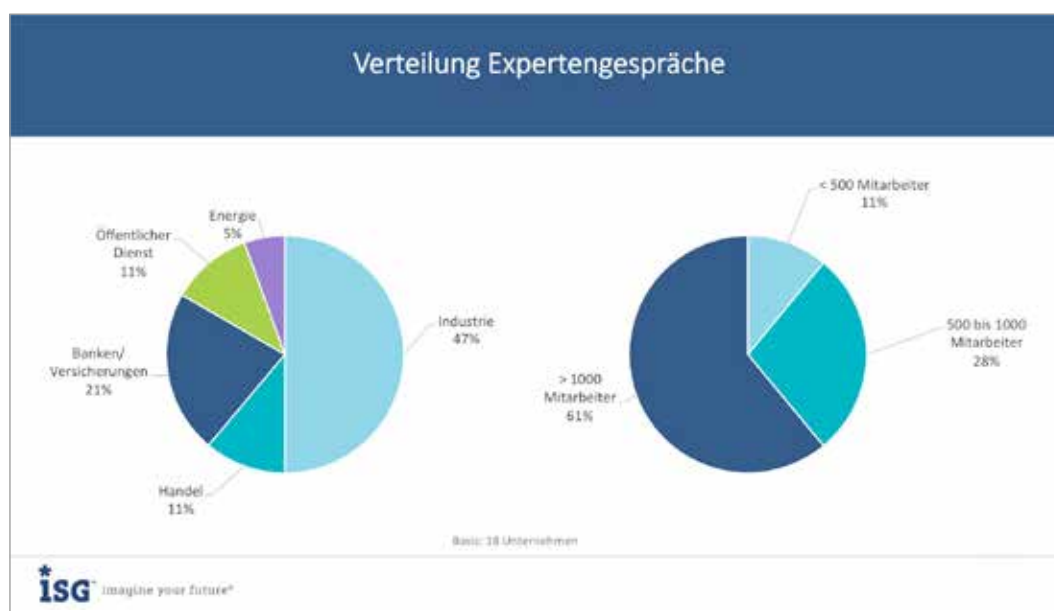


Abbildung 2: Verteilung Expertengespräche

Um die Überlegungen und Analysen in diesem Handbuch empirisch zu untermauern, wurde seitens der ISG Germany eine Umfrage unter Experten für *Compliance* durchgeführt. Die Ergebnisse dieser Umfrage werden in den entsprechenden Kapiteln vorgestellt. Einzelne Zitate aus den Interviews sind als „Expertenstatements“ kenntlich gemacht.

Befragt wurden mittels Interviews und Fragebögen 18 Experten für *Compliance* und Datenschutz aus den Sektoren Industrie und Dienstleistungen. Die oben stehenden Grafiken zeigen die Verteilung.

KAPITEL 3

15

DIE DIGITALE TRANSFORMATION UND DIE *CLOUD*

3. DIE DIGITALE TRANSFORMATION UND DIE *CLOUD*

In diesem Kapitel wird zunächst die digitale Transformation mit ihren strategischen Implikationen für Organisationen betrachtet. In Abschnitt 3.1 werden die Auswirkungen aktueller Trends auf Geschäftsprozesse, deren *Workflows* sowie auf Arbeitsplätze und -techniken diskutiert. Durch die Entwicklungen der digitalen Transformation entstehen auch neue Herausforderungen, auf die in Abschnitt 3.2 genauer eingegangen wird. Das mobile Arbeiten erfordert beispielsweise zahlreiche Richtlinien, die etwa im Gerätemanagement umgesetzt werden müssen. In Abschnitt 3.3 wird die Frage nach dem strategischen Nutzen der digitalen Transformation gestellt. Ergebnisse einer Expertenbefragung zeigen hier, welche Technologien und Trends im Vordergrund stehen. Dabei zeigt sich, dass die *Cloud* mit ihrer zentralen Bevorratung von Daten und Diensten für die digitale Transformation in Organisationen strategisch und technologisch von elementarer Bedeutung ist.

3.1 Entwicklungen der digitalen Transformation

Die Entwicklung immer neuer Technologien geht mit fortlaufenden Veränderungen in Unternehmen und Organisationen einher und ebnet den Weg für die Digitalisierung. Das bedeutet, dass immer mehr bisher analoge Prozesse und Abläufe auf IT-Technologien basieren, was die Effizienz in Organisationen beträchtlich steigern kann. Dass die digitale Transformation einen enormen strategischen Nutzen für Organisationen und Unternehmen haben kann, zeigen die zahlreichen bestehenden Anwendungen, etwa im Bereich *Cloud Computing*, mobiles Arbeiten und dem Internet der Dinge. Nach wie vor entstehen in diesen und anderen Bereichen stetig neue, innovative Geschäftsideen. Die Trends und Technologien der digitalen Transformation bedeuten aus Sicht von Unternehmen und Organisationen also vor allem auch fortlaufenden Wandel.

3.1.1 Technologien, Trends und Ziele

Im Rahmen der von ISG durchgeführten Umfrage unter Experten aus Unternehmen unterschiedlicher Branchen und Größen wurde die Wichtigkeit von Technologien und Trends der digitalen Transformation für die Unternehmen bzw. Organisationen der Experten thematisiert. Die folgende Grafik veranschaulicht die Expertenmeinungen.



Abbildung 3: Bedeutung der Digitalisierung für Unternehmen

Die Umfrageergebnisse lassen auf eine hohe bis sehr hohe Wertschätzung der Trends und Technologien der digitalen Transformation durch die befragten Experten schließen. Diese eindeutige Stimmungslage verwundert nicht in Anbetracht der vielfältigen Geschäfts- und Optimierungsmöglichkeiten, die sich durch die digitale Transformation für Unternehmen ergeben.

Ausgehend von den technischen Möglichkeiten lassen sich für Anbieter, Mitarbeiter und Kunden neue Ziele definieren, die mit der digitalen Transformation erreicht werden können:

- Ganz neue Produkte und Dienstleistungen werden entwickelt oder bereits bestehende Produkte und Dienstleistungen werden vereinfacht, verschlankt, um neue Funktionen erweitert oder in ihrem Ablauf optimiert.
- Produktion und Abläufe werden komplett automatisiert, auch so weit gehend, dass sich Prozesse über Unternehmensgrenzen hinweg selbsttätig durch die Kommunikation zwischen Maschinen steuern und Ereignisse auslösen.
- Kunden werden stärker in Produkte und Dienstleistungen eingebunden. Dies führt zu einem verbesserten Kundenerlebnis, schnelleren Prozessen und einer verbesserten Kundenbindung.
- Kosten werden verringert, weil überflüssige manuelle Anteile von *Workflows* von IT-Systemen übernommen und Fehler verringert werden.

Expertenstatement: Die Digitalisierung ist für unseren Onlineversand und im Rahmen der Anbindung der externen Partner und der unternehmensübergreifenden Integration der IT-Systeme sehr relevant. Das Käuferverhalten hat sich zunehmend geändert und erfordert schnellere Reaktionszeiten. Die interne IT muss aber erst noch „enabled“ werden.

Nutzníeßer der digitalen Transformation sind dabei alle Beteiligten: Unternehmer können schnell auf die Wünsche ihrer Kunden reagieren und ad hoc innovative Produkte und Dienstleistungen in den Markt bringen und skalieren, aufbauend auf einer automatisierten Wertschöpfungskette. Mitarbeiter werden von lästigen und zeitfressenden Tätigkeiten entlastet und können sich um die wesentlichen Dinge, die Optimierung und Weiterentwicklung ihrer Arbeit kümmern. Und die Kunden profitieren von den auf ihren Bedarf zugeschnittenen Angeboten, möglicher Individualisierung („*build to customer order*“) sowie einer verbesserten Interaktion mit dem Anbieter. Das alles ist möglich bei sinkenden Kosten und höherem Durchsatz, also einer Anhebung der Gesamtgeschwindigkeit.

Analystenfazit:

Nutzníeßer der digitalen Transformation sind Unternehmer, deren Mitarbeiter sowie die Kunden.



Im Folgenden werden die wichtigsten Trends und Entwicklungen im Zusammenhang mit der digitalen Transformation diskutiert.

3.1.2 Digitalisierung von Geschäftsprozessen

Eine besonders deutlich zu erkennende Veränderung durch die digitale Transformation betrifft Geschäftsprozesse (*Workflows*), also Vorgänge und Abläufe innerhalb von Unternehmen und Behörden. Allgemeine Geschäftsprozesse und ihre durch die Ablauforganisation definierten Arbeitsabschnitte und Arbeitsschritte wurden bisher durch die IT-Technologie nur bedingt unterstützt. Viele Geschäftsprozesse, insbesondere auch in der Interaktion mit Dritten, hatten viele Brüche und auch Nicht-IT-Anteile, die dann oft manuell bearbeitet werden mussten. Ein einfaches Beispiel dafür sind E-Mails, die zwar optimiert durch die IT transportiert werden, dann aber so lange im Eingangskorb eines Benutzers verbleiben, bis dieser sie liest und bearbeitet. Eine weitere, aber auch entscheidende Dimension manueller Vorgänge sind deren Fehleranfälligkeit und Sicherheitsrisiken, beispielsweise durch *Phishing*-Mails, Betrugs- oder Erpressungs-Trojaner. Zudem führt ein immer größer werdendes E-Mail-Aufkommen zur Überlastung von Mitarbeitern, was eine steigende Fehlerquote mit sich bringen kann. Der Ablauf der Verarbeitung von E-Mails ist folglich nicht effizient.

Expertenstatements: Moderne Technologien ermöglichen durchgängige Geschäftsprozesse und die flexible und echtzeitgetriebene Verarbeitung von Daten. Dadurch wird das *Business* gefördert. Was noch fehlt, sind durchgängige Standards.

Viele Geschäftsprozesse sind momentan noch zu individuell und noch nicht über *Workflows* abgebildet. Hier fehlt es noch vielfach an der notwendigen Reife und Standardisierung.

Bei der Digitalisierung von Geschäftsprozessen geht es darum, zu teure, überflüssige, fehleranfällige oder sicherheitskritische manuelle Anteile am *Workflow* nicht nur durch die IT zu unterstützen, sondern durch die IT abzubilden und somit zu automatisieren. Das ist eine neue Qualität. Durch die IT werden standardisierte Abläufe sowie benutzerfreundliche und eingabengestützende Schnittstellen zur Verfügung gestellt, die auch nicht-IT-affine Mitarbeiter und Kunden ansprechen. Ferner können diese *Interfaces* durch weitgehende Automatisierung und Autonomisierung so optimiert werden, dass die oben aufgezählten Schwächen einfach wegfallen. Wichtig dabei ist, dass die neue Technik Akzeptanz bei Anwendern und Kunden findet, denn wenn die Wünsche, die sich mit der digitalen Transformation verbinden, unerfüllt bleiben, bleibt auch der wirtschaftliche Erfolg aus. Klar ist jedoch auch, dass Unternehmen und Organisationen gerade durch die neuen technologischen Ansätze dazu in die Lage versetzt werden, geräteunabhängige Lösungen mit situationsangepassten und sicheren Schnittstellen zu Menschen und Maschinen bereitzustellen. Wer sich strategisch mit dem Mehrwert der unterschiedlichen neuen Technologien auseinandersetzt, kann frühzeitig die Weichen für eine prosperierende Zukunft stellen.



Analystenfazit:

Im Zuge der digitalen Transformation werden *Workflows* standardisiert und automatisiert. Dadurch werden Fehler vermieden, Angriffe verhindert und Geschäftsprozesse optimiert.

3.1.3 Digitaler und mobiler *Workspace*

Mit der digitalen Transformation ändern sich nicht nur Geschäftsprozesse und *Workflows*, sondern auch die Arbeitsplätze der beteiligten Mitarbeiter. Bei einer zentralen Datenhaltung, den notwendigen Benutzerschnittstellen sowie gesicherten Verbindungen mit rollenbasierten Zugriffen besteht kein Grund mehr, seine Arbeit im Büro oder im Homeoffice zu erledigen. Prinzipiell können Mitarbeiter an jedem Ort der Welt mit jedem denkbaren Endgerät ihren Teil der Arbeit erledigen, genauso wie Partner und insbesondere Kunden. Benutzerfreundliche Schnittstellen, die es Kunden ermöglichen, selbst in Prozesse einbezogen zu werden, sind gerade eine Grundlage der Digitalisierung.

Solche Kundenschnittstellen und digitalen Arbeitsplätze werfen aus Sicht von Sicherheit und *Compliance* entscheidende Fragen auf, insbesondere bei Auswahl und Absicherung von Endgeräten. Prinzipiell sollten neben Desktop-Systemen und Laptops, deren Sicherheit man mit klassischen Methoden gut in den Griff bekommen kann, auch Smartphones und Tablets eingesetzt werden können, inklusive *BYOD*-Geräten. Die Anforderungen an das Endgeräte-Management und die Endpunkt-Security steigen unter diesen Vorgaben stark an.

Kunden- und Benutzer-*Interfaces*, mit denen die manuellen *Workflow*-Anteile abgewickelt werden, müssen sich an diese digitalen Arbeitsplätze anpassen lassen. In der Regel werden die Schnittstellen über webbasierte Applikationen zur Verfügung gestellt. Da gerade im Bereich der Darstellung von Webinhalten viel Erfahrung mit der Skalierung auf unterschiedliche Endgeräte besteht, sollten sich hier keine großen Anpassungsprobleme ergeben.

3.1.4 Veränderte Arbeitstechniken

Digitale Arbeitsplätze führen zu anderen Arbeitstechniken. Standardisierte, webbasierte Benutzerschnittstellen werden anders bedient als typische Anwendungen, wie man sie aus dem Büroalltag kennt. Natürlich wird von den betroffenen Mitarbeitern erwartet, dass sie sich an die neuen Arbeitstechniken gewöhnen und die gewohnte Leistung für das Unternehmen erbringen. Durch die Standardisierung fallen aber auch „Rüstzeiten“ beim Wechsel von einer Anwendung in eine andere weg, etwa durch zentrale Bereitstellung oder Updates. Durch eine kontextbezogene Plausibilisierung wird zudem die Fehlerquote bei der Eingabe gesenkt.

Bei den Themen Sicherheit und *Compliance* sind solche Standardisierungen ein großer Vorteil. Richtlinien müssen nicht mehr an jede Applikation angepasst werden. Zudem ergeben sich Synergieeffekte bei der technischen Erzwingung der Umsetzung von Richtlinien, da die Technik im Hintergrund weniger Plattformen als bisher bedienen muss. Ein gutes Beispiel in dieser Hinsicht ist das *Single-Sign-on* (SSO), bei dem in klassischen Büroumgebungen eine Unzahl von Plattformen und Anwendungen bedient werden muss. Bei webbasierten Anwendungen lässt sich SSO viel einfacher und zuverlässiger implementieren.

3.1.5 Internet der Dinge

Das Internet der Dinge (*IoT*) ist ein ganz bedeutender Antrieb für die digitale Transformation. Wenn sich Geräte untereinander verständigen, also Maschinen mit Maschinen, so setzt das vollautomatisierte *Workflows* voraus. Das *IoT* ist somit Paradebeispiel und Testfeld für neue Technologien zugleich.

Am *IoT* kann auch gesehen werden, wohin die Reise bei der digitalen Transformation führt. *IoT*-Lösungen sind in der Regel cloudbasiert, d. h. die einzelnen Systeme halten nur wenige Daten lokal vor und sind über das Internet erreichbar und steuerbar. Die Verarbeitung der Signale von *IoT*-Geräten über zentrale Datenspeicherung unter Mithilfe von selbstlernenden Systemen und künstlicher Intelligenz macht die Zukunft des *IoT* aus.

Über die *Cloud* und standardisierte Schnittstellen können die unterschiedlichsten Geräte in ein *IoT* eingebunden werden und miteinander sowie mit zentralen Stellen kommunizieren. Die übergeordneten *Workflows* sind in der Regel relativ starr vorgegeben, denn einen großen Entscheidungsspielraum wird den angeschlossenen Geräten nicht gegeben. Die eigentliche Intelligenz sitzt in den *Workflows* in der *Cloud*. Die Geräte haben nur eine lokale Sicht auf die Vorgänge und arbeiten ausschließlich mit den für sie relevanten Daten, die sie über eine abgesicherte Kommunikation untereinander und über die zentrale Steuerung erhalten.

Um die digitale Transformation umzusetzen, kommen moderne Technologien wie mobiles Computing, plattform- und geräteübergreifende Applikationen und Kommunikation, *Big-Data*-Analysen, selbstlernende Systeme sowie künstliche Intelligenz zum Einsatz. Diese Technologien sind mit ihrem Anspruch an Kapazität, Skalierbarkeit, Flexibilität, Funktionalität und Rechenleistung in einem wirtschaftlich vertretbaren Ausmaß nur noch über *Cloud*-Angebote realisierbar. Man kann die *Cloud* daher geradezu als Basistechnologie für die digitale Transformation bezeichnen.



Analystenfazit:

Die Anforderungen der digitalen Transformation an *Workflows*, Arbeitsplätze und -techniken lassen sich durch den verstärkten Einsatz von *Cloud*-Technologien erfüllen. Das Internet der Dinge ist ohne *Cloud* sogar undenkbar.

3.2 Herausforderungen der digitalen Transformation

Durch die digitale Transformation entstehen ganz neue Anforderungen, etwa an die Einhaltung von Regularien. Der schnelle technologische Wandel muss dabei auf strategischer, technologischer und organisationaler Ebene erkannt und berücksichtigt werden. Vor allem Unternehmen und Behörden, die sich bisher nicht mit der Digitalisierung beschäftigt haben, müssen umlernen und sich auf schnell veränderliche technische und organisatorische Rahmenbedingungen einstellen. Die Einhaltung regulatorischer Anforderungen (*Compliance*) spielt eine besondere Rolle, um Fortschritt und Wandel unter Berücksichtigung potenzieller Risiken umzusetzen.

Im Detail wird das Zusammenspiel von *Compliance* und der digitalen Transformation Gegenstand späterer Kapitel sein. Im folgenden Abschnitt werden zunächst Herausforderungen aus *Compliance*-Sicht für die bereits aufgegriffenen Technologien und Trends der digitalen Transformation diskutiert.

3.2.1 Kooperation durch übergreifende *Workflows*

In vielen Fällen erstrecken sich *Workflows* über den Einflussbereich einer Organisation hinaus. Beispiele sind hier *Just-in-time*-Beziehungen zwischen Automobilherstellern und ihren Zulieferungen oder *Self-Service*-Portale von Stadtverwaltungen. Unter *Compliance*-Gesichtspunkten können sich hier Überschneidungen oder Widersprüche auftun, etwa wenn die beiden Partner unterschiedliche Anforderungen erfüllen müssen oder der Status von *Compliance*-Umsetzungen des Partners unbekannt ist.

Bei den beiden Beispielen aus der Automobilindustrie oder öffentlichen Portalen kann die Erfüllung von *Compliance*-Anforderungen mittels SLAs oder Nutzungsbestimmungen erzwungen werden. Schwieriger wird es, wenn beide Seiten inkompatible Anforderungen haben – etwa wenn ein Unternehmen einen Lieferanten in China hat und zu den *Compliance*-Anforderungen des deutschen Unternehmens der Einsatz bestimmter zertifizierter Verschlüsselungsverfahren gehört.

3.2.2 Mobilität, Flexibilität, Sicherheit

Mit digitalen und mobilen Arbeitsplätzen werden klassische Perimeterschutzkonzepte außer Kraft gesetzt. Daten, Systeme und Arbeitsplätze befinden sich nicht mehr in Bereichen, die unter der (vermeintlichen) Kontrolle eines Unternehmens oder einer Behörde stehen. Die Arbeitsplätze können überall auf der Welt sein, etwa in öffentlichen Hotspots oder in fremden Kundennetzwerken. Die Verbindung zu den eigenen Systemen, also der Transport der Daten zu den Arbeitsplätzen, erfolgt über Netze, die ebenfalls nicht der Kontrolle der eigenen Organisation unterliegen und über deren Sicherheit meist keine Aussage möglich ist.

Die Arbeitsplätze selbst wandeln sich kontinuierlich. Natürlich wird es immer noch die klassischen Firmenarbeitsplätze geben, die gemäß strengen Richtlinien vorkonfiguriert und mit sehr beschränkten Benutzerrechten ausgeliefert werden. Doch es werden in zunehmendem Maße auch privat angeschaffte Tablets, Smartphones oder andere Geräte angebunden werden, bei denen die Firma oder die Behörde nur eingeschränkte Konfigurationsmöglichkeiten hat. Damit geht einher, dass sich das Augenmerk immer mehr auf die Daten, deren Klassifizierung und deren angepassten Schutz verlagert. Infrastruktur und Geräte selbst werden zweitrangig. Zudem wird die Unterscheidung zwischen privaten und geschäftlichen Daten immer mehr an Relevanz gewinnen, insbesondere bei einer parallelen Verarbeitung in verschiedenen Endgeräten und Anwendungen (Kommunikation, Social Media, Adressdaten etc.).

Expertenstatement: Bei der digitalen Transformation werden mehr kritische Daten über Unternehmensgrenzen transferiert und verarbeitet. Auf diese wird über immer mehr Systeme und Devices zugegriffen. Damit erhöhen sich exponentiell die möglichen Angriffspunkte sowie auch die Gefahr zum falschen Umgang mit Daten.

Trotz dieser Randbedingungen müssen unsichere Netzwerke und Geräte die eigenen *Compliance*-Anforderungen erfüllen. Die *Compliance* und die betriebswirtschaftliche Aufgabe, geschäftseigene Daten und die Verfügbarkeit von Diensten zu schützen, befruchten sich dabei gegenseitig. Wenn etwa als *Compliance*-Vorgabe die Umsetzung des Informationssicherheitsstandards ISO 27001 erforderlich ist, sind beispielsweise verschlüsselte Verbindungen und die ausreichende Absicherung von Endgeräten nicht nur eine lästige Erfüllung der Pflicht, sondern dienen dem Schutz relevanter sensibler Geschäftsdaten und damit dem eigenen Geschäftszweck.

3.2.3 Schnelle und automatisierte Kommunikation

Zum Wesen von vollautomatisierten *Workflows* gehört die schnelle, automatisierte und kontinuierliche Kommunikation. Lediglich bei den manuellen *Workflow*-Anteilen wird dieser Prozess für die Zeit der Bearbeitung angehalten, um nach der Interaktion wieder fortgesetzt zu werden.

Schnelle und automatisierte Kommunikation schafft unter Sicherheitsgesichtspunkten Herausforderungen. Wenn in der Automatik ein Fehler auftritt, ist es kaum noch möglich, diesen manuell zu korrigieren und Folgeerscheinungen zu unterbinden. Dies bedeutet, dass in automatisierten *Workflows* die Fehleranfälligkeit und -wahrscheinlichkeit extrem gering gehalten und Sicherheitsmaßnahmen entsprechend ganzheitlich angewendet werden müssen. Diese geringen Fehlerraten kann man nur erreichen, wenn an vielen Stellen des *Workflows* automatische Überprüfungen auf Plausibilität und Einhaltung von Vorgaben stattfinden. Die Sicherheitsmaßnahmen müssen eine durchdachte Architektur haben und Möglichkeiten zur Überwachung und Reaktion umfassen.

In diesem Punkte gehen Sicherheit und *Compliance* Hand in Hand. Denn auch die Einhaltung von *Compliance*-Anforderungen muss weitgehend automatisiert werden. Dazu sind Mechanismen nötig, mit denen die Umsetzung von Richtlinien entweder erzwungen wird oder zumindest eine Kontrolle mit der Möglichkeit zum Abbruch des *Workflows* im Falle von *Compliance*-Verletzungen gegeben ist.

3.2.4 Die Welt der Maschinen

Das Internet der Dinge stellt eine der größten Herausforderung für die *Compliance* dar. Denn hier geht es um eine Welt, in der Maschinen und Geräte *Workflows* weitgehend selbstständig abwickeln und der menschliche Einfluss – abgesehen von der initialen Konfiguration – gering ist. Das gilt besonders bei selbstlernenden autonomen Systemen.

In dieser rein technischen, von Maschine zu Maschine gesteuerten Welt müssen *Compliance*-Vorgaben in technische Vorgaben übersetzt und im *IoT* an die beteiligten Systeme verteilt werden. Eine Welt, in der Roboter, intelligente Stromzähler, Router und Switches, Heizungsthermostate, Kameras, Kühlschränke und fast beliebige andere Systeme zu Hause sind, ist mit ihren Sensoren, Akteuren und Events extrem heterogen. Die Übersetzung von Vorgaben in gerätespezifische Richtlinien stellt deshalb eine Herausforderung dar, die noch nicht ansatzweise gelöst ist. Dies gilt ebenso für Kontrollen, ob die Richtlinien tatsächlich auch umgesetzt worden sind. Die Erzwingbarkeit von Regeln muss daher zukünftig integraler Bestandteil von *IoT*-Geräten sein.

Da Logik, Systeme und Daten von *IoT*-Netzwerken in aller Regel zentral in einer *Cloud* gehalten werden, lassen sich einige *Compliance*-Anforderungen in der *Cloud* bündeln. Dies trifft etwa in den Bereichen Sicherheit und Datenschutz zu, da sämtliche Aspekte der physischen und logischen Datensicherheit sowie die Umsetzung von Datenschutzrichtlinien in der *Cloud* umgesetzt werden können, also beispielsweise der Perimeterschutz, der Einsatz von Verschlüsselungstechnologien und die Klassifizierung von Daten. Leider existieren bisher für die große Masse an möglichen und bereits verfügbaren *IoT*-Geräten kaum Regularien und Standards, was eine flächendeckende Durchsetzung sicherer und zuverlässiger Technologien und die strategische Planung für Anbieter erschwert.

3.3 Strategische Aspekte der digitalen Transformation

Bei der Betrachtung der Vorteile und Herausforderungen wurde bereits angedeutet, dass die digitale Transformation aus strategischer Sicht eine hohe Relevanz für Unternehmen und Organisationen hat. Dies belegt auch die ISG-Umfrage unter Experten aus unterschiedlichen Unternehmen und Branchen. Im nun folgenden Abschnitt soll dieses grobe Bild weiter verfeinert und um konkretere Erkenntnisse ergänzt werden. Am Ende steht eine klare Übersicht darüber, welche Technologien die digitale Transformation prägen und welche strategischen Implikationen dies für Unternehmen und Organisationen mit sich bringt.

3.3.1 Technologische Entwicklungen

In der Praxis bietet es sich an, Anwendungen und Daten zentral zu halten und die Zugriffsvergabe und Handhabung an zentral definierbare Richtlinien zu knüpfen. Diese Richtlinien müssen bereits bei der Prozessgestaltung berücksichtigt werden, damit ein Anwender Zugriff nur auf die Daten und Systeme erhält, die er für seine *Workflows* auch wirklich braucht. Eine Voraussetzung hierfür ist die zentrale Definition und Überwachung von Sicherheitsrichtlinien. Außerdem muss eine zentrale und automatisierte Steuerung der Vergabe von Zugriffsberechtigung und Handhabung für die angepasste Verwendung von Ressourcen wie Geräten und Diensten möglich sein.

Welche konkreten Auswirkungen haben diese und weitere Entwicklungen auf die strategische Haltung von Unternehmen und Organisationen gegenüber der digitalen Transformation, ihren Technologien und Trends? Im Rahmen der ISG-Umfrage wurden Experten nach deren Stellenwert befragt.



Abbildung 4: Bedeutung von Technologien für die digitale Transformation

Expertenstatements: Insbesondere *IoT*- und *Cloud*-Technologien haben maßgeblichen Einfluss auf die Weiterentwicklung unseres Geschäfts, steigern die Wettbewerbsfähigkeit und ermöglichen neue Geschäftszweige. Auf der anderen Seite wird der Wettbewerb aber auch deutlich globaler und härter.

Über *IoT*, *Cloud* und *Mobile* haben wir komplett neue Möglichkeiten, flexibel, skalierend und plattformbasierend auf die dynamischen Marktentwicklungen zu reagieren. Die Reaktionsgeschwindigkeit in der IT wird deutlich schneller.

Generell zeigt sich in der Umfrage eine recht hohe Wertschätzung einiger technologischer Trends der digitalen Transformation. *Big Data Analytics*, *Mobile Computing* und das Internet der Dinge zeigen hohe Zustimmungswerte unter den Experten. In einem Punkt sind sich jedoch die befragten Experten nahezu einig: *Cloud Computing* hat einen sehr hohen strategischen Stellenwert für die Unternehmen bzw. Organisationen der befragten Experten. Woher der hohe wahrgenommene Stellenwert der *Cloud* im Meinungsbild der befragten Experten kommt, wird im Weiteren noch genauer untersucht.

3.3.2 *Cloud* als Basistechnologie

Auf zahlreichen Anwendungsgebieten hat sich *Cloud Computing* in den letzten Jahren insbesondere aufgrund der kostengünstigen und skalierbaren Bereitstellung virtualisierter Ressourcen als Schlüsseltechnologie für die zentralisierte Bereitstellung von Daten und Systemen etabliert. *Cloud*-Anbieter stellen ihren Kunden ein immer größer werdendes Portfolio an Diensten bereit, was die Möglichkeiten in Bezug auf Anwendungsszenarien, aber auch im Hinblick auf die individuelle Konfiguration und Steuerung der Daten- und Systemlandschaft stetig erweitert.

Die digitale Transformation kann getrost als „Killer-Applikation“ für die *Cloud* bezeichnet werden. Ohne die *Cloud* in ihrer Funktion als zentrale und standardisierte Plattform für Daten und Systeme sind zentrale Anliegen der digitalen Transformation nur schwer umsetzbar. Hierzu zählen nicht nur automatisierte *Workflows* und das Internet der Dinge, sondern auch die Durchsetzung von Sicherheitsrichtlinien und ein nachhaltiges Gerätemanagement. Hierdurch wird etwa ein nachhaltiges Konzept zur mobilen Arbeit überhaupt erst möglich. Auch Institutionen oder Organisationen, die sich eine Nutzung der *Cloud* bislang gar nicht vorstellen konnten, müssen sich die Frage stellen, ob sie die digitale Transformation ohne *Cloud*-Technologie überhaupt durchführen können.

Expertenstatement: Die für die digitale Transformation notwendige Skalierbarkeit ist mit vernünftigem Aufwand nur über *Cloud*-Technologien herzustellen. Zum Teil fehlt es aber noch an der notwendigen Standardisierung sowie international gleich hohen Sicherheitsstandards und Gesetzen.

Ob die Daten in einer öffentlichen, privaten oder hybriden *Cloud* abgelegt sind, spielt für die Funktionalität eines automatisierten *Workflows* zunächst keine Rolle. Unter *Compliance*-Gesichtspunkten, wie zum Beispiel Sicherheitsanforderungen, kann die Auswahl eines bestimmten *Cloud*-Modells allerdings eine große Bedeutung haben. Im folgenden Kapitel wird das Thema *Compliance* zunächst allgemein analysiert. Anschließend wird das Thema im Zusammenhang mit den Entwicklungen und Chancen der digitalen Transformation und des *Cloud* Computings betrachtet.

Analystenfazit:

Umsetzbarkeit und Erfolg der digitalen Transformation stehen und fallen mit der fortlaufenden Umsetzung regulatorischer Anforderungen. Die *Cloud* stellt hierfür eine Basistechnologie dar, da sie für den Informationsaustausch innerhalb der *Workflows* erforderlich ist und sich mit ihrer Hilfe viele *Compliance*-Anforderungen erfüllen lassen.

4. COMPLIANCE UND DIE DIGITALE TRANSFORMATION

In Abschnitt 4.1 dieses Kapitels wird definiert, was *Compliance* ist und was sie für die digitale Transformation bedeutet. Anhand der compliancerelevanten Thematik der Informationssicherheit wird verdeutlicht, vor welchen Herausforderungen Organisationen im Moment stehen, aber auch welche Chancen aktuelle Technologien und Trends für die *Compliance* darstellen können. Dabei wird auch deutlich, dass die Umsetzung von *Compliance*-Anforderungen nicht nur zur Erfüllung von regulatorischen Anforderungen dient, sondern einen direkten Nutzen für Informationssicherheit und Datenschutz innerhalb der eigenen Firma oder Behörde hat.

Darauf aufbauend wird in Abschnitt 4.2 ein Blick auf die Frage geworfen, welche Chancen die Technologien und Trends der digitalen Transformation – allen voran *Cloud Computing* – für die *Compliance* in Unternehmen bieten können und welche positiven Auswirkungen hieraus auch auf den Geschäftserfolg resultieren können. Basierend auf den resultierenden Kernaussagen wird in Abschnitt 4.3 ein Ausblick auf die Rolle und Gestalt von *Compliance* in einer immer stärker digitalisierten Welt gegeben.

4.1 *Compliance* – eine Einführung

Sprach man in der Vergangenheit über *Compliance* im Kontext von IT, so gab es einen relativ breiten Konsens darüber, welche Arten von Regularien gemeint waren. In vielen Fällen ging und geht es bis heute um Themen wie Sicherheit und Datenschutz. Die digitale Transformation erweitert den Fokus, da immer mehr bisher kaum oder gar nicht IT-gestützte Prozesse durch IT-Technologien erfasst werden. Es lohnt sich also, vor der inhaltlichen Auseinandersetzung mit *Compliance* im Kontext der digitalen Transformation eine terminologische Auseinandersetzung mit den unterschiedlichen *Compliance*-Begriffen vorzunehmen. So fällt es im Anschluss leichter, ein Verständnis für die Veränderungen zu entwickeln, die sich im Zuge der digitalen Transformation auch für den strategischen Wert von *Compliance* aus geschäftlicher Sicht ergeben.

4.1.1 Begriffe und Definitionen

Dazu soll zunächst eine Definition des Begriffs „*Compliance*“ im Spannungsfeld der digitalen Transformation vorgenommen werden. Eine Spezifizierung von allgemeinen und IT-spezifischen *Compliance*-Begriffen ist da hilfreich. Die folgenden Begriffe finden so auch in vielen anderen Werken Anwendung:

Compliance im Allgemeinen bezeichnet Aktivitäten, um ein regelkonformes Verhalten zu erlangen und Hilfsmittel zur Abbildung der Unternehmenslage bereitzustellen. Dabei geht es nicht nur um Gesetzeskonformität, sondern auch um das Einhalten von unternehmensinternen Richtlinien, die wiederum auf Best Practices – also empfohlenen Richtlinien und Standards – basieren können. Das schafft einen Verhaltenskodex, der dem Aufbau einer Vertrauensbasis im geschäftlichen Umgang dient. Dieser Kodex gilt zwischen Geschäftspartnern, im Verhältnis zu Kunden, innerhalb des Unternehmens sowie als Vorgabe für Dienstleister jeglicher Art.

IT Compliance beschäftigt sich als Teilbereich der *Compliance* schwerpunktmäßig mit denjenigen *Compliance*-Anforderungen, welche die IT-Systeme eines Unternehmens oder einer Organisation betreffen.

Der Begriff **Corporate Compliance** soll im Rahmen dieses Handbuchs zur Abgrenzung von der IT Compliance dienen. Mit Corporate Compliance sind also die Compliance-Anforderungen gemeint, welche vom Begriff der IT Compliance nicht erfasst werden.

Wie wirken sich digitale Transformation und *Cloud Computing* auf den strategischen Umgang mit dem Themenkomplex *Compliance* aus und wie kann *Compliance* in Anbetracht größerer technologischer und organisatorischer Umbrüche in Unternehmen und Organisationen erfolgreich gestaltet werden? Im folgenden Teil dieses Kapitels wird ein strategischer Ausblick auf Herausforderungen und Chancen der digitalen Transformation in Bezug auf *Compliance* gegeben.

4.1.2 IT Compliance und Corporate Compliance – Grenzen verschwimmen

Man könnte meinen, dass es sich bei der digitalen Transformation um ein Thema primär im Spannungsfeld der *IT Compliance* handelt. Die in Kapitel 5 beschriebenen Anwendungsfälle der digitalen Transformation zeigen aber, dass diese Annahme zu kurz greift. Im Zuge der Digitalisierung bisher analoger Geschäftsprozesse und *Workflows* werden auch Anforderungen wichtig, die bisher der *Corporate Compliance* zugeordnet wurden. Mit der digitalen Transformation wandert auch die Umsetzung von *Corporate-Compliance*-Anforderungen zusammen mit den Geschäftsprozessen mehr und mehr in die digitale Welt. Die IT muss Geschäftsprozesse und *Compliance*-Anforderungen abbilden und umsetzen. Das betrifft auch Geschäftsprozesse, die bisher keinen oder nur einen minimalen Anteil an IT hatten.

Expertenstatements: Bei der *Compliance* verliert man aufgrund ihrer Komplexität den Überblick. Der Wandel (Technologie und Organisation) erfolgt in den Branchen und Unternehmen sehr dezentral und in unterschiedlichen Geschwindigkeiten. Das erhöht die Risiken und erschwert die unternehmensweite und -übergreifende Sicherstellung des Themas.

Die aktuell größten Risiken für die *Compliance* ergeben sich durch die hohe Anzahl von heterogenen und komplexen Anforderungen und Regularien. Damit entsteht die Gefahr von Verstößen und Nichteinhaltung.

Analystenfazit:

Im Zuge der digitalen Transformation werden die Bereiche der *Compliance*, die noch ohne IT auskommen, immer kleiner werden. Die IT unterstützt zunehmend Geschäftsprozesse und *Compliance*-Lösungen, die bisher keinen oder nur einen minimalen Anteil an IT hatten.

Als Beispiel für diese Umsetzung von *Corporate-Compliance*-Anforderungen über IT soll eine Bank dienen, die einen neuen Prozess zur Bekämpfung von Geldwäsche aufsetzen will. Banken sind nach dem Geldwäschegesetz verpflichtet, den Missbrauch ihrer Finanzdienstleistungen für Geldwäsche zu bekämpfen. Dabei setzen Banken ein umfassendes Maßnahmenbündel um, das etwa Identitätsprüfungen von Einzel- und Unternehmenskunden, Erfassung und Bewertung von Geldwäscherisiken und eine Überprüfung des Kundenverhaltens hinsichtlich verdächtiger Verhaltensmuster beinhaltet. Auch wenn heute bereits *Workflows* und *Workflow*-Anteile der Prozesse in Banken durch IT-Systeme unterstützt werden, ist ein erheblicher Ressourceneinsatz nötig, um die zahllosen Transaktionen zu überwachen.¹

Basierend auf *Big-Data*-Analysetechniken überwachen Banken Transaktionen und Risiken in Echtzeit. Damit steigern sie ihre Transparenz gegenüber Strafverfolgungs- und Aufsichtsbehörden. Gleichzeitig werden Ressourcen eingespart, da weniger Mitarbeiter für die Überwachung von Transaktionen benötigt werden. Greift die Bank auf eine *Cloud*-Lösung zurück, kann zusätzlich eine hohe Skalierbarkeit der für die Analysen verfügbaren Rechenressourcen und somit eine hohe Flexibilität bezüglich möglicher steigender Anforderungen an die IT-Infrastruktur erreicht werden.

Der Wandel, von dem die *IT und Corporate Compliance* im Zuge der digitalen Transformation erfasst wird, hat auch größere Auswirkungen auf die Aufgaben der *Compliance*-Verantwortlichen in Unternehmen und Behörden. Zu diesem Schluss kommt der Großteil der von ISG befragten Experten. Die folgende Grafik veranschaulicht das Meinungsbild zu dieser Frage.



Abbildung 5: Aufgaben *Compliance*-Verantwortliche

Die Auswirkungen dieser Entwicklung auf den Umgang einzelner Mitarbeiter mit dem Thema *Compliance* schätzen die befragten Experten allerdings mehrheitlich als eher gering ein, was in der folgenden Grafik veranschaulicht wird.

¹ Vgl. FAQ des Bankenverbands zum Thema Geldwäsche

<https://bankenverband.de/fachthemen/steuern/fragen-und-antworten-zum-thema-geldwaesche/>

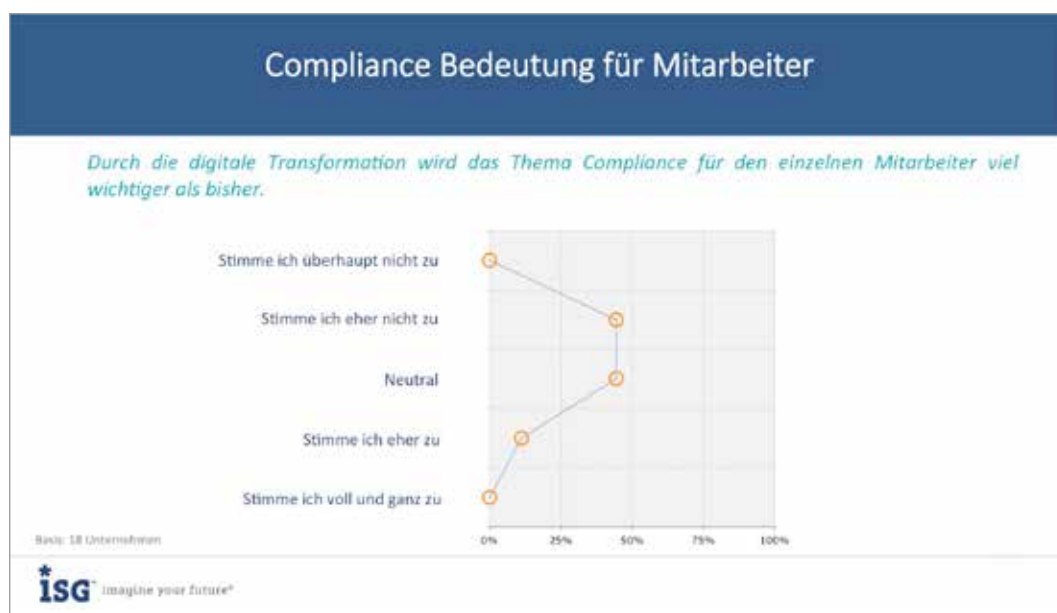


Abbildung 6: Compliance-Bedeutung für Mitarbeiter

Die Einhaltung regulatorischer Anforderungen scheint in Anbetracht tiefgreifender technologischer und organisatorischer Veränderungen also primär eine Frage des Managements und der Prozessgestaltung zu sein. Da *Compliance*-Anforderungen in Form von Regeln automatisch in die Benutzerschnittstellen integriert werden, befindet sich der Anwender bereits in einem *Compliance*-Rahmen, in den die Umsetzung eines großen Teils der Regeln bereits eingearbeitet ist.

4.1.3 IT Compliance – eine Frage der Sicherheit?

Derzeit lässt sich ein kontinuierlicher Anstieg der Anforderungen an Sicherheit und den Schutz von Informationen erkennen, der sich nicht auf *Cloud*-Anbieter und -Infrastrukturen beschränkt. Seit dem Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 (NIS Verweis) gelten nicht nur für Betreiber kritischer Infrastrukturen, sondern auch für Betreiber von Webangeboten erhöhte technische und organisatorische Sicherheitsmaßnahmen zum Schutz von Kundendaten und IT-Systemen. Das Bundesdatenschutzgesetz verlangt zudem konkret die Umsetzung technischer und organisatorischer Maßnahmen zum Schutz von Kundendaten bei der IT-gestützten Verarbeitung. 2018 wird mit der *General Data Protection Regulation (GDPR)* auf EU-Ebene eine einheitliche Regulierung zum Datenschutz aller EU-Bürger getroffen werden, die auch den Datenexport in Länder außerhalb der EU reguliert.

Das Thema der *IT Compliance* hängt daher nach wie vor stark mit Fragen des Datenschutzes und der Informationssicherheit zusammen. Gerade beim Einsatz von *Cloud*-Lösungen ist Sicherheit ein zentrales und viel diskutiertes Thema. Dies unterstreichen auch die Ergebnisse einer auf Microsoft Insights publizierten Studie zur Zukunft der Informationssicherheit, für die 365 führende IT-Manager aus der Wirtschaft befragt wurden. Die Studie schlägt den Bogen von aktuellen Angriffen über die Nutzung von *Cloud*-Diensten bis hin zu Anforderungen an *Cloud*-Anbieter.

Die Ergebnisse besagen, dass fast ein Viertel aller befragten Unternehmen in den vergangenen zwölf Monaten von einer Cyberattacke betroffen war. In diesem Zusammenhang gibt die Studie auch Aufschluss darüber, welche Bedrohungen für den Schutz von Daten von besonderer Bedeutung sind. Auf den vorderen Plätzen landen dabei *Phishing*-Angriffe, *Social Engineering*, *Malware* mit Zugriff auf schützenswerte Daten und sogenannte *Advanced Persistent Threats (APT)*, also raffinierte, zielgerichtete und technologisch hoch entwickelte Angriffe, die mit großem Aufwand betrieben werden.

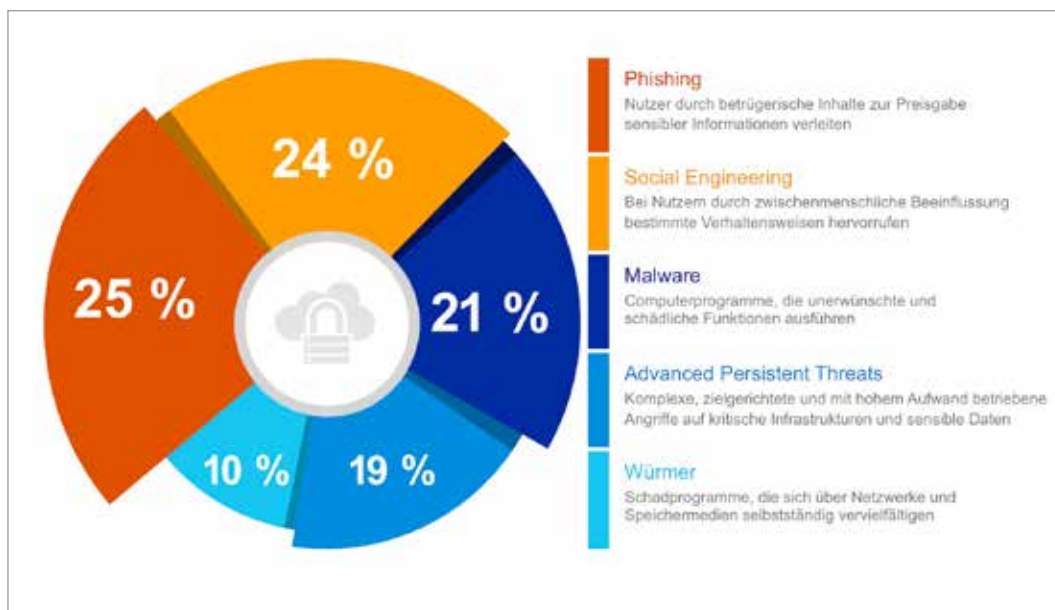


Abbildung 7: Microsoft Insights Studie – Bedeutung von Cyberbedrohungen

Die Darstellung stellt das aktuelle Bedrohungsszenario deutlich dar. Die weiteren Fragen der Studie ermitteln unter Berücksichtigung dieser Bedrohungen, wie es mit der aktuellen Nutzung von *Cloud*-Diensten aussieht und welche Anforderungen an die Anbieter gestellt werden.

Die Ergebnisse der Studie besagen, dass aktuell 31 % der Befragten die *Cloud* für mehr als 50 % und 48 % der Befragten die *Cloud* für weniger als 25 % ihrer operativen Aktivitäten verwenden.

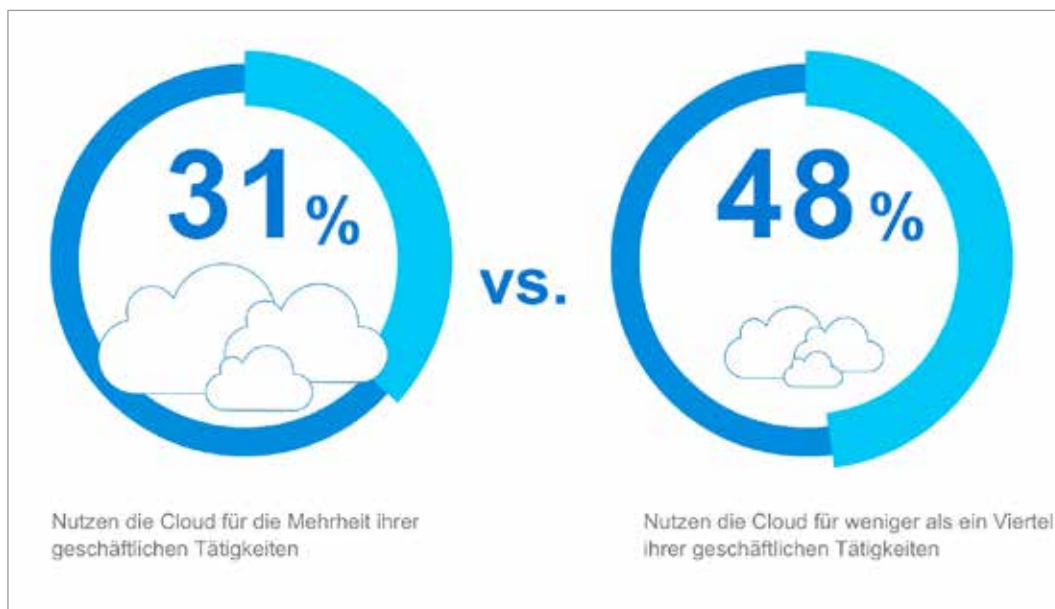


Abbildung 8: Microsoft Insights Studie – Nutzung von *Cloud Computing*

In knapp einem Drittel der befragten Unternehmen leistet die *Cloud* also bereits einen erheblichen Anteil bei Erbringung und Bereitstellung von IT-Infrastruktur und Diensten. In knapp der Hälfte der befragten Unternehmen wird immerhin für weniger als ein Viertel der operativen Aktivitäten auf *Cloud*-Dienste zurückgegriffen. Die Nutzung von *Cloud*-Diensten ist also bei den meisten Befragten Bestandteil des normalen Tagesgeschäfts.

Auf welche Eigenschaften legen die befragten Unternehmen bei der Wahl des *Cloud*-Anbieters in Folge besonderen Wert? Die Frage nach den wichtigsten Qualitäten eines *Cloud*-Anbieters liefert recht aussagekräftige, eindeutige Ergebnisse.

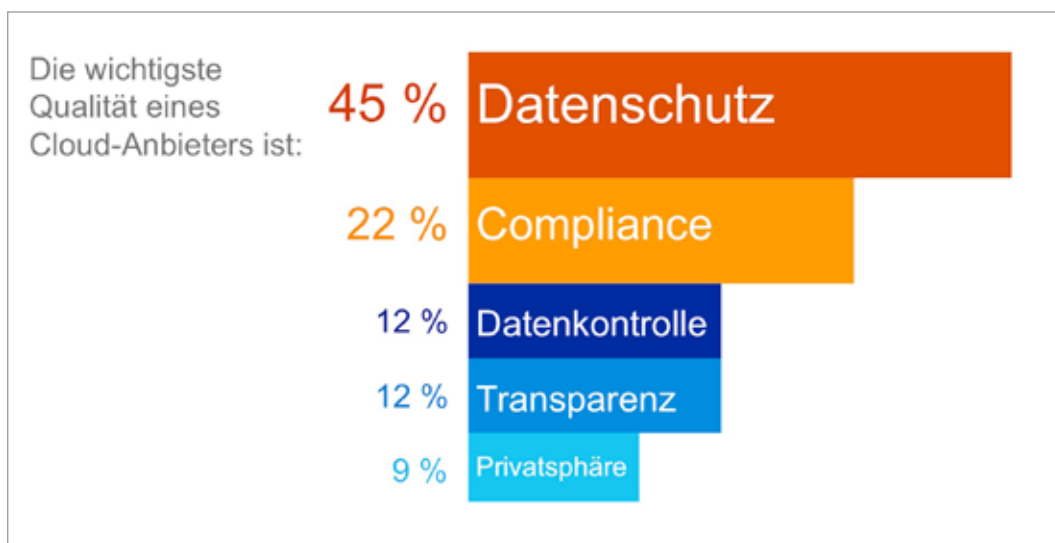


Abbildung 9: *Microsoft Insights Studie* – Bedeutung von Qualitäten eines *Cloud*-Anbieters

Mit einer hohen Zustimmung von 45 % überragt das Thema *Datenschutz* die Diskussion. 22 % der befragten Unternehmen messen zudem dem Thema *Compliance* eine hohe Bedeutung bei. Mit jeweils 12 % runden die Themen *Datenkontrolle* und *Transparenz* das Feld der Kriterien ab.

Für Unternehmen und Organisationen, die den Schritt in Richtung digitale Transformation gehen wollen, haben diese Fragen einen hohen Stellenwert. Es sind Kriterien erforderlich, nach denen Anbieter verglichen und auf Kompatibilität mit den eigenen *IT-Compliance*-Anforderungen geprüft werden können. In der Regel werden Referenzkunden, eigene Erfahrungen mit dem Anbieter, vor allem aber Zertifizierungen nach anerkannten Standards als Entscheidungskriterien genutzt. Mittlerweile gibt es einige Standards und Zertifizierungen, die sich an den Einsatz von *Cloud*-Lösungen richten und über die sich cloudspezifische *Compliance*-Anforderungen abbilden lassen.

Einige Beispiele:

- Der *Cloud Computing Compliance Controls Catalogue (C5)*, ein Prüfschema des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- ISO 27001 spezifiziert Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung des Kontexts einer Organisation
- ISO 27017, ein Maßnahmenkatalog für Informationssicherheit in *Cloud*-Diensten
- ISO 27018, ein Maßnahmenkatalog für den Schutz personenbezogener Informationen, die im Rahmen einer Auftragsdatenverarbeitung in öffentlichen *Cloud*-Diensten verarbeitet werden

Auch aus Anbietersicht spielen Einhaltung, Zertifizierung und regelmäßige Auditierung von Standards bei der Erreichung geschäftlicher Ziele eine wichtige Rolle. Solche Maßnahmen schaffen Transparenz im Hinblick auf das Sicherheitsniveau der *Cloud*-Dienste und spielen somit eine wichtige Rolle beim Gewinnen des Vertrauens potenzieller Kunden. Im Wettbewerb um Kunden stellen die Einhaltung von Standards und die fortlaufende und frühzeitige Bereitstellung transparenter und unabhängiger Belege in Form von Audits und Zertifizierungen einen wichtigen Differenzierungspunkt dar. Abgesehen davon liegt es auch im Interesse von *Cloud*-Anbietern, ihre eigene Infrastruktur und die verarbeiteten Daten vor teuren und geschäftsschädigenden Angriffen zu schützen. Der Erfolg der *Cloud* steht und fällt also mit den Antworten, die *Cloud*-Anbieter auf die Sicherheits- und Datenschutzerfordernungen ihrer Kunden finden, basierend auf entsprechenden Maßnahmen.

Compliance stellt also – gerade im Bereich Sicherheit und Datenschutz – mitnichten nur eine kostspielige, aber strategisch irrelevante Notwendigkeit dar. Vielmehr muss die Frage erlaubt sein, ob und wie Kunden bei der Nutzung von *Cloud*-Diensten Synergien nutzen, ihren Umgang mit *Compliance* effizienter gestalten und so auch einen Beitrag zur Steigerung des **Geschäftserfolges** leisten können.



Analystenfazit:

Ein *Cloud*-Anbieter muss sich mit den Themen Sicherheit, *IT Compliance* und Transparenz beschäftigen. *Compliance* stellt mitnichten nur eine kostspielige, aber strategisch irrelevante Notwendigkeit dar. Die Umsetzung von *Compliance*-Anforderungen wird immer auch einen Beitrag zur Steigerung des Geschäftserfolges leisten.

4.2 *Compliance* und *Cloud*: Risiko oder Chance?

Aus Sicht von *Cloud*-Anbietern stellt die Umsetzung der *Compliance*-Anforderungen von Kunden einen wichtigen Wettbewerbsfaktor dar. Gleichzeitig gelten zahlreiche Regularien für vom Anbieter betriebene *Cloud*-Systeme und für kundenbetriebene *On-Premises*-Systeme gleichermaßen. Es besteht also nicht nur die Möglichkeit, die Umsetzung von *Compliance*-Anforderungen durch bestimmte *Cloud Services* zu unterstützen. Die Umsetzung, Auditierung und Zertifizierung von *Compliance*-Anforderungen kann in einigen Fällen sogar direkt in die Zuständigkeit des Anbieters fallen. Die folgenden Abschnitte geben Aufschluss über die Chancen, welche mit einer *Cloud*-Nutzung für die *Compliance* einhergehen.

4.2.1 *Compliance* als Strategie für *Cloud*-Anbieter

Eine Voraussetzung für die Erzielung von Synergieeffekten ist, dass zwei Akteure in einer Art und Weise zusammenwirken, die für den Gesamtnutzen förderlich ist. Im Kontext der Themen Datenschutz und Informationssicherheit wurde bereits verdeutlicht, dass die Einhaltung von Kundenanforderungen aus Anbietersicht einen wichtigen Wettbewerbsfaktor darstellt.

Setzt man nun einen generischen, übergreifenden Blickwinkel auf das Verhältnis zwischen

Anbieter- und Kundenanforderungen in Bezug auf *Compliance* voraus, so lassen sich zunächst zwei Feststellungen treffen:

1. Auf dem Markt der *Cloud*-Anbieter existieren zahlreiche Angebote, die Lösungen für die umfassenden geschäftlichen und regulatorischen Anforderungen von Kunden aus unterschiedlichen Branchen versprechen.
2. Viele *IT-Compliance*-Anforderungen, die *Cloud*-Anbieter erfüllen müssen, müssen in gleicher Weise auch von IT-Systemen und IT-Diensten anderer Unternehmen erfüllt werden – ganz egal, ob es sich dabei um *On-Premises*- oder *On-Purpose*-Dienste handelt.

Was bedeutet das für Unternehmen und Organisationen, die *Cloud*-Dienste nutzen oder nutzen möchten und dabei ihre eigenen *Compliance*-Anforderungen umsetzen müssen? Zum einen unterliegen *Cloud*-Anbieter – als Anbieter von IT-Diensten – selbst hohen *Compliance*-Anforderungen. Darüber hinaus messen *Cloud*-Anbieter dem Thema *Compliance* als Verkaufsargument eine immens hohe Bedeutung bei. Dies zeigt sich nicht nur in den bereits erwähnten ständig wachsenden Dienstportfolios, mit denen *Cloud*-Anbieter ihre Kunden bei der Einhaltung allgemeiner wie branchenspezifischer Anforderungen unterstützen möchten. Auch beständige hohe Investitionen, etwa im Bereich Sicherheit und Datenschutz, verdeutlichen dieses Interesse der Anbieter.

Aus Kundensicht bedeutet dies, dass die *Cloud* Nutzenpotenziale bei der Einhaltung von *Compliance*-Anforderungen freisetzt. Anbieter setzen das technologische Innovationspotenzial der *Cloud* in Dienste um, welche den *Compliance*-Anforderungen von Unternehmen und Organisationen gerecht werden. Dabei orientieren sich *Cloud*-Anbieter an technischen und organisatorischen Standards, welche auch für Kunden eine hohe Relevanz haben können. Diese Sichtweise wird auch durch die Ergebnisse der Expertenumfrage von ISG unterstützt.

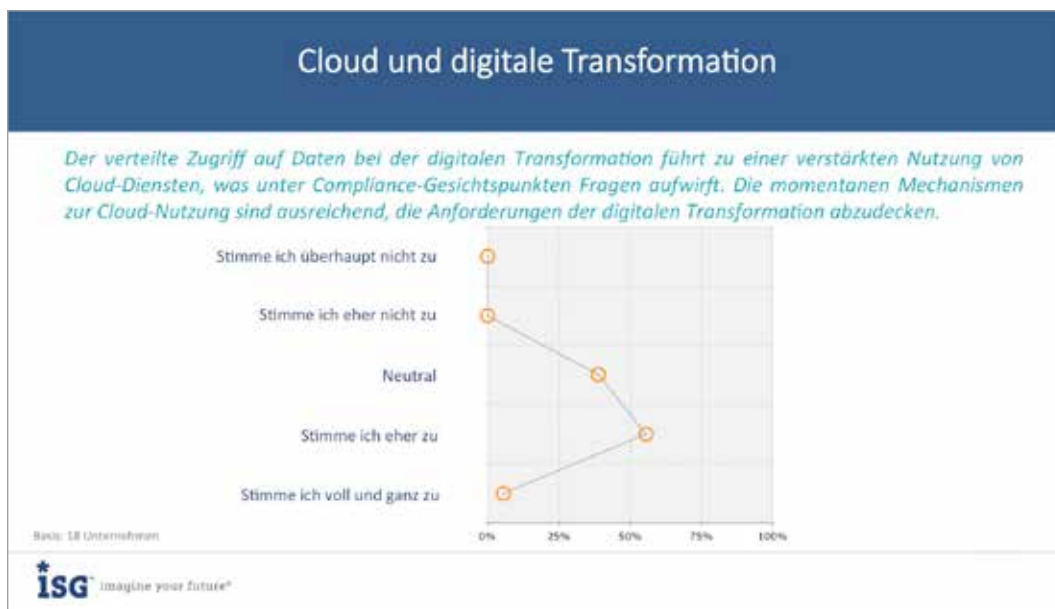


Abbildung 10: *Cloud* und digitale Transformation

Die in der oben abgebildeten Grafik dargestellten Ergebnisse lassen darauf schließen, dass die befragten Experten sich durch die momentan vorhandenen Mechanismen und Technologien der *Cloud* mehrheitlich gut für die Herausforderungen der digitalen Transformation gewappnet sehen. Gleichzeitig lässt sich erkennen, dass *Compliance*-Probleme, die sich direkt auf die Nutzung von *Cloud*-Diensten zurückführen lassen, eine eher geringe Rolle spielen.

In den folgenden Abschnitten des Kapitels wird thematisiert, welche Chancen die *Cloud* in Bezug auf die Einhaltung regulatorischer *Compliance*-Anforderungen bietet und wie Kunden das Potenzial der *Cloud* für die Einhaltung regulatorischer Anforderungen und letztlich auch zur Steigerung des **Geschäftserfolges** nutzen können.

4.2.2 Wie unterstützt die *Cloud* die Umsetzung von *Compliance*?

Durch die digitale Transformation werden vermehrt *Workflows* etabliert, welche unternehmens- bzw. organisationsübergreifend gestaltet sind und somit die Einhaltung von *Compliance*-Anforderungen unterschiedlicher Unternehmen bzw. Organisationen notwendig machen. Im Rahmen der ISG-Expertenumfrage wurden auch Lösungsansätze für den Umgang mit heterogenen *Compliance*-Anforderungen thematisiert. Die Experten messen nicht nur technischen Lösungen, sondern vor allem auch organisatorischen Maßnahmen eine hohe Bedeutung speziell bei der Gestaltung regelkonformer organisationsübergreifender *Workflows* bei, was in der folgenden Grafik deutlich wird.



Abbildung 11: Digitalisierung von *Workflows*

Darüber hinaus sehen die befragten Experten in der Standardisierung und Automatisierung von Prozessen und *Workflows* durch technische Maßnahmen mehrheitlich eine Chance zur Vereinfachung der Einhaltung von *Compliance*-Anforderungen. Die folgende Grafik zeigt das Meinungsbild zu dieser Frage.

Cloud Computing und die daraus hervorgehenden Technologien schaffen ein breites und stetig wachsendes Spektrum an Lösungen zur Festlegung und Umsetzung von *Compliance*-Anforderungen. Ein Ansatz, der es erlaubt, *Compliance*-Anforderungen an zentraler Stelle zu definieren, umzusetzen, zu erzwingen und zu überwachen, wird im Folgenden grob skizziert:

- Über ein zentrales *Repository* werden *Compliance*-Anforderungen definiert. Das kann in Form von abstrakten Vorgaben („muss dem deutschen Datenschutz genügen“) oder auch mittels detaillierter Richtlinien bzw. technischer Vorgaben erfolgen.
- Daten können in der *Cloud* nach ihrem Schutzbedarf klassifiziert und in unterschiedlichen Zonen verarbeitet werden. Ihre Verwendung kann dann in den verschiedenen *Workflows* gesteuert und kontrolliert werden.
- Die Umsetzung von *Compliance*-Anforderungen erfolgt in der *Cloud* durch die Erzwingung der Richtlinien gemäß der Definition im *Repository*.

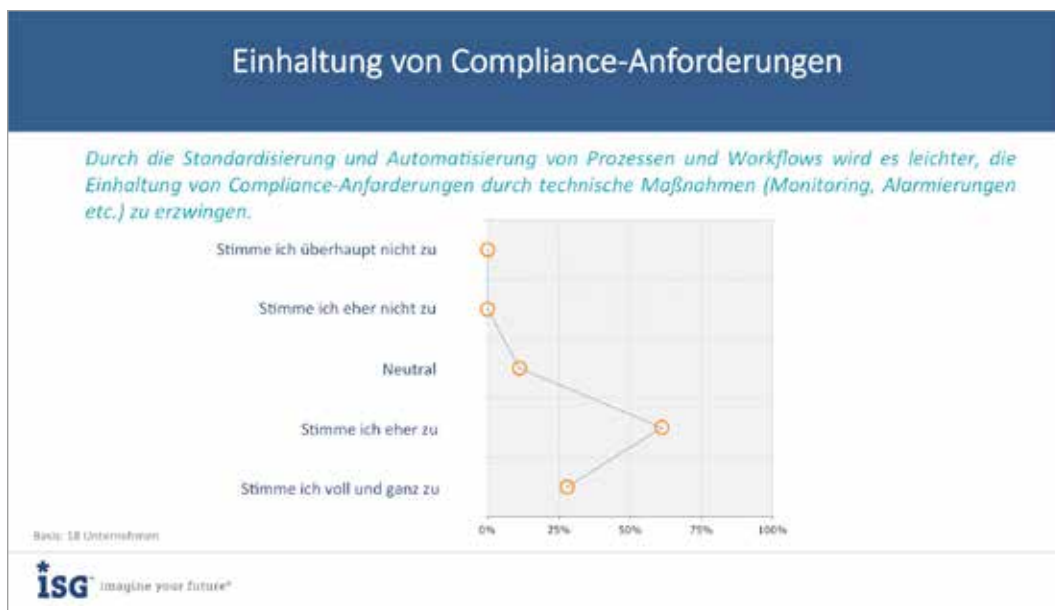


Abbildung 12: Expertenmeinung – Bedeutung von Standardisierung und Automatisierung für Compliance

Das Leistungsspektrum von *Cloud*-Anbietern beinhaltet häufig Prozesse und Tools, die Unternehmen bei der Erfüllung regulatorischer Anforderungen unterstützen und sie damit von der Eigenentwicklung derartiger Lösung befreien. Hierzu zählen beispielsweise das Management von Vorfällen, die Risikobeurteilung, die rollenbasierte Zugriffsverwaltung oder die Überwachung von Zugriffen auf Daten und Systeme. *Cloud*-Anbieter können häufig auch Ressourcen oder *Best Practices* zum Erhalt weiterführender Zertifizierungen auf Basis eines *Cloud*-Dienstes bereitstellen. Nicht zuletzt tragen auch die Technologien der digitalen Transformation selbst zur Verbesserung der Einhaltung von *IT-Compliance*-Anforderungen bei. Sogenannte *Managed Security Services* unterstützen gerade kleinere Unternehmen mit skalierbaren Sicherheitslösungen aus der *Cloud*, mit denen das Schutzniveau von Daten und Systemen beträchtlich gesteigert werden kann. Auch *Big-Data*-Analysen leisten bei der Suche nach Schwachstellen oder der Analyse von Vorfällen einen wichtigen Beitrag. Durch *Machine-Learning*-Algorithmen können Angriffsmuster erkannt und Abhilfe geleistet werden.

Durch *Cloud*-Technologie bereitgestellte Dienste versetzten Unternehmen in die Lage, die Umsetzung und Überwachung technischer und organisatorischer *Compliance*-Anforderungen zu automatisieren und somit effizient und effektiv zu gestalten.

Wenn Unternehmen untereinander und auch *Cloud*-Anbieter vergleichbare oder gleiche *Compliance*-Anforderungen einhalten müssen, dann lassen sich Synergieeffekte freisetzen, da durch die *Cloud*-Nutzung die technischen und organisatorischen Umsetzungen vom *Cloud*-Anbieter sichergestellt und nachgewiesen werden. Im folgenden Abschnitt werden die Chancen solcher Nutzenpotenziale diskutiert.

4.2.3 *Compliance as a Service?* Leichter als gedacht!

In den vorherigen Abschnitten wurde offensichtlich, warum für *Cloud*-Anbieter die Abbildung wichtiger Regularien und Standards in ihren Diensten ein für den eigenen geschäftlichen Erfolg wichtiges Anliegen darstellt. Audits und Zertifizierungen kommt in diesem Kontext sowohl für *Cloud*-Anbieter als auch für Unternehmen, die ihre Dienste in die *Cloud* verlagern, eine sehr wichtige Rolle zu.

In vielen Fällen endet der Nutzen, den die Auslagerung von Diensten in die *Cloud* für die Einhaltung von Regularien bietet, noch nicht an dieser Stelle. Während beim *On-Premises*-Betrieb von IT-Diensten gerade im Zuge der technischen Bereitstellung auf Software- und Hardwareebene zahlreiche Standards erfüllt und Zertifizierungen abgelegt werden müssen, obliegt die Zuständigkeit hierfür bei der *Cloud*-Nutzung meist dem Anbieter. Zwar findet kein direkter Transfer der Verantwortung für die Einhaltung von *IT-Compliance*-Anforderungen vom *Cloud*-Kunden zum *Cloud*-Anbieter statt. Allerdings fällt die Umsetzung der relevanten technischen und organisatorischen Anforderungen dem *Cloud*-Anbieter zu, welche beim *On-Premises*-Betrieb in die Zuständigkeit des Kunden fallen würden. Das Ausmaß dieses Transfers von Zuständigkeiten hängt in erster Linie vom *Cloud*-Dienstmodell ab. Eine umfassende Darstellung dieser Zusammenhänge in den unterschiedlichen Modellen wird in Kapitel 7 gegeben.

Aus Kundensicht ergibt sich hieraus der Vorteil, dass nicht nur die Aufgabe der Umsetzung des eigentlich eingekauften Dienstes selbst, sondern auch zahlreicher technischer und organisatorischer Schutzmaßnahmen an den *Cloud*-Anbieter abgegeben wird, die er sonst selbst in seiner eigenen Umgebung erfüllen müsste. Auch die regelmäßigen Audits müssen vom *Cloud*-Anbieter angestoßen werden und dienen dem Kunden sowohl als Grundlage für die Akzeptanz des Anbieters als auch seinem eigenen Nachweis. Der Kunde erspart sich damit fortlaufende Kosten für die Bereitstellung und Instandhaltung einer aktuellen technischen Sicherheitsinfrastruktur. Organisatorische Aufgaben wie die Bereitstellung von Notfallprozessen oder Schulungen für Mitarbeiter werden ebenfalls verlagert. Gerade bei kleineren Unternehmen bedeutet dies nicht nur eine starke Entlastung von kosten- und arbeitsintensiven Aufgaben sowie dediziertem Personal, sondern oft auch die Erzielung eines höheren Schutzniveaus. Datenschutz und Sicherheit stellen für *Cloud*-Anbieter sehr wichtige Differenzierungsmerkmale dar, weshalb diese in der Regel signifikante Investitionen in diesem Bereich tätigen.

Aus Sicht von *Cloud*-Kunden entfällt zudem die Notwendigkeit neuer Zertifizierungen bei Ausweitung oder Veränderung des Portfolios der IT-Dienste. Während bei einer *On-Premises*-Bereitstellung von IT-Diensten die Einhaltung von Anforderungen über Audits und Zertifizierungen stets neu sichergestellt werden muss, führen *Cloud*-Anbieter diese Audits und Zertifizierungen grundsätzlich für einen Großteil ihrer Dienste durch. Möchte nun ein Kunde das Portfolio seiner IT-Dienste ausbauen oder umstrukturieren, entfällt beim *Cloud*-Bezug der Dienste der erneute Nachweis der Erfüllung der Anforderungen, da dieser fortlaufend vom *Cloud*-Anbieter erbracht wird. Veränderungen am IT-Dienstportfolio können also auch deswegen aus der *Cloud* deutlich effizienter und flexibler durchgeführt werden.

Nicht zuletzt ergibt sich zudem der Effekt, dass gerade bei Unternehmen, die in einer Wertschöpfungskette zusammenarbeiten und *Compliance*-Vorgaben des Herstellers unterliegen, diese einfach und direkt über den *Cloud*-Anbieter nachweisen können. Gegebenenfalls hat der Hersteller auch *Cloud*-Anbieter vorselektiert, die die Einhaltung der Vorgaben nachweisen können.

4.3 Resümee: *Compliance* wird digitaler und standardisierter

Neben den bereits erörterten technischen Möglichkeiten ergeben sich auch organisatorische Vorteile und strategische Chancen. *Compliance*-Maßnahmen auf Anbieterseite, aber auch die Bereitstellung immer besserer und innovativerer Dienste zur Umsetzung der technischen und organisatorischen *Compliance* auf Kundenseite stellen für *Cloud*-Anbieter einen wichtigen Wettbewerbsfaktor dar.

Zudem bietet die *Cloud*, wie im vorigen Abschnitt beschrieben, weitere Synergieeffekte zwischen Anbieter und Kunden, wenn sich deren *Compliance*-Anforderungen überschneiden. Die Umsetzung von Standards, Audits und Zertifizierungen fallen dann in den Zuständigkeitsbereich des Anbieters.

Festhalten lassen sich also abschließend nicht nur fortlaufende Verbesserungen der technischen und organisatorischen Umsetzung von *Compliance* durch die digitale Transformation und speziell die *Cloud*. Unternehmen können zusätzlich Synergien durch das Auslagern der Zuständigkeit für Standardisierung, Auditierung und Zertifizierung von Prozessen und Infrastrukturen erzielen.

All das geschieht vor dem Hintergrund, dass immer neue *Compliance*-Anforderungen und Anwendungsszenarien von der Innovationsspirale der digitalen Transformation erfasst werden. Denn wie in Kapitel 4.1 beschrieben wurde, profitieren auch Anforderungen, Prozesse und *Workflows* der *Corporate Compliance* immer mehr von IT-Unterstützung – basierend auf Technologien und Trends der digitalen Transformation.

Expertenstatement: Ein Vorteil, den man sich von der *Cloud* versprechen kann, ist der automatische Nachweis der Einhaltung bestimmter Vorschriften. Wenn meine Zulieferer eine bestimmte *Cloud*-Plattform verwenden, dann weiß ich, dass diese Wertschöpfungskette eine bestimmte Anforderung auf jeden Fall erfüllt, wenn diese durch den *Cloud*-Anbieter so bereitgestellt wird, z. B. Anforderungen an die Sicherheit. Ist der *Cloud*-Anbieter in diesem Bereich zudem zertifiziert, dann wird der Nachweis dieser *Compliance* noch einfacher. Das erleichtert meine Auditierung und reduziert meinen Aufwand. Ein wichtiger Punkt ist auch die Weiterentwicklung der *Compliance*-Maßnahmen, die dann gleichzeitig auf die gesamte Wertschöpfungskette wirken und durch den *Cloud*-Anbieter selbst verfolgt werden, getrieben durch den Wettbewerb. Das verschafft mir Vorteile, ohne dass ich mich selbst darum bemühen muss, und ohne unmittelbare zusätzliche Kosten.



Analystenfazit:

Neue IT-Technologien ermöglichen die Gestaltung von Prozessen, mit denen die Einhaltung von *Compliance*-Anforderungen sichergestellt und überwacht wird, auch in Bereichen, in denen bisher keine oder kaum IT zum Einsatz kam.

KAPITEL 5

39

COMPLIANCE UND GESCHÄFTSERFOLG VERBINDEN – EIN MODELL

5. COMPLIANCE UND GESCHÄFTSERFOLG VERBINDEN – EIN MODELL

Neben den technologischen Entwicklungen und Trends ist nach wie vor die Frage nach der strategischen Umsetzung von *Compliance* relevant. Im Abschnitt 5.1 wird der Ansatz „*Governance, Risk Management und Compliance (GRC)*“ beschrieben, der das Thema *Compliance* in eine unternehmensweite, strategische Perspektive der Unternehmensführung einbettet. Überträgt man den *GRC*-Ansatz in den Kontext der Umsetzung von *Compliance*, so stehen die Einhaltung regulatorischer Anforderungen und der geschäftliche Erfolg in keinem Widerspruch zueinander. Vielmehr lassen sich gemeinsame Ziele erkennen, die auch durch strategische Aspekte der digitalen Transformation als fortlaufendem Treiber für technologische und organisatorische Veränderung geprägt sind.

In Abschnitt 5.2 wird – basierend auf sechs gemeinsamen Zielen regulatorischer und geschäftlicher Anforderungen – sukzessive ein Modell entwickelt und beschrieben, das Kernbereiche und Handlungsfelder regulatorischer und geschäftlicher Anforderungen formuliert.

5.1 *Compliance* als strategischer Ansatz

Die vorhergehenden Kapitel haben Aufschluss darüber gegeben, wie sich Entwicklungen und Trends der digitalen Transformation auf Organisationen und Unternehmen auswirken. Das Verhältnis zum zweiten großen Themenkomplex – der *Compliance* – stellt sich dabei ambivalent dar: Zum einen wirkt sich die digitale Transformation auf die Art und Weise aus, wie regulatorische Anforderungen erfüllt werden. Zum anderen ergeben sich aus den neuen Technologien, Trends und Geschäftsmodellen neue Anforderungen, die auch für die IT bisher wenig relevante Bereiche erfassen.

Governance, Risk Management und Compliance stellt einen bekannten Ansatz dar, der *Compliance* sowohl strategisch als auch operativ einordnet. Dieser Ansatz stellt, wie schon in der Vorgängerversion des Handbuchs, die Basis für die Entwicklung eines Modells dar, das die gemeinsamen Ziele von *Compliance* und Geschäftserfolg unter Beachtung aktueller Entwicklungen strukturiert darstellt.

5.1.1 *Compliance* aus *Governance*-Sicht

Auf der anderen Seite steht die Betrachtung von *Compliance* aus *Governance*-Sicht. *Compliance* wird dabei als Mittel zur Führung einer Organisation verstanden, mit dem Ziel, die *Compliance* kontinuierlich zu verbessern. Damit trägt sie direkt zum **Geschäftserfolg** des Unternehmens oder der Behörde bei. Diese Verbesserung beschränkt sich nicht nur auf die beteiligten Informationssysteme, sondern hilft gleichzeitig, Transparenz und Verfügbarkeit von Informationen zu erhöhen sowie die Kosten für Beschaffung und Auswertung von Informationen zu senken. Damit wird die Effizienz von Geschäftsprozessen sowie der gesamten Organisation gesteigert. Das Management kann schneller auf Geschäftsdaten zugreifen und seine Aufgaben bei der Lenkung der Organisation besser wahrnehmen.

Ein Ansatz, der geschäftliche und regulatorische Aspekte der *Compliance* verbindet, schlägt zwei Fliegen mit einer Klappe. Neben der Erfüllung externer Anforderungen trägt *Compliance* direkt dazu bei, Geschäftsprozesse zu optimieren und letztlich die eigene Organisation zum Erfolg zu führen.

Diese doppelte Funktion von *Compliance* spielt in diesem Handbuch eine wichtige Rolle. Das im Folgenden vorgestellte *Compliance*-Modell berücksichtigt beide Aspekte und hilft, die regulatorischen und geschäftlichen Anforderungen zu erfassen und umzusetzen. Diese

strategische Funktion der *Compliance* lässt sich besonders gut im Kontext von *Governance* und *Risk Management* aufzeigen. Die konkrete Anwendung des Modells wird dann in Kapitel 6 beschrieben.

5.1.2 GRC – Governance, Risk Management und Compliance

Das Einhalten von Regelungen (*Compliance* im allgemeinen Sinn) ist keine isolierte Maßnahme, sondern fällt in den größeren Zusammenhang von *Governance*, *Risk Management* und *Compliance* (GRC). GRC bildet die strategische Klammer für verschiedenste Aufgaben, die die Lücke zwischen Unternehmensstrategie und -zielen einerseits und dem operativen Tagesgeschäft auf der anderen Seite schließt. GRC ist keine Technologie, sondern Ansatz und Prozess, um Synergien zwischen Geschäftszielen und Regularien zu realisieren.

Governance dient als Oberbegriff für die verantwortungsvolle Führung von Unternehmensbereichen oder eines ganzen Unternehmens. Dazu gehören das Festlegen von Zielen und Verantwortlichkeiten, die Definition von Aktivitäten und Kontrollmechanismen sowie die Ressourcenplanung und das Einbetten in einen Risikomanagementprozess. Im Rahmen der Steuerung auf allen Ebenen liegt dabei ein besonders starkes Gewicht auf dem Ausrichten der Zielsetzungen an der Unternehmensstrategie – etwa im Bereich der *IT Governance*.

Risk Management ist ein systematischer, prozessorientierter Ansatz, um Risiken zu identifizieren, zu analysieren, zu bewerten, zu behandeln und zu überwachen. Eine wichtige Zielsetzung liegt daher im Verständnis von Bedrohungen, Schwachstellen und Risiken für das Unternehmen, im Abbau von Risiken durch entsprechende Maßnahmen oder der Anstrengung, das Restrisiko so gut wie möglich einzuschätzen. Die Liste potenzieller Risikobereiche ist lang und reicht von der Sicherheit für Mitarbeiter, Gebäude, Produktionsanlagen und Informationen über Technologie- und Projektrisiken bis hin zu Risiken im Umfeld von *Compliance* und Kriminalität, Ethik und Kultur, Geopolitik und Klima – um nur eine Auswahl zu nennen.

Ein mit Blick auf GRC gut aufgestelltes Unternehmen

- erhöht die Effizienz und Wirksamkeit von organisatorischen und technischen Prozessen
- schützt die Reputation und die Werte des Unternehmens
- schafft Transparenz gegenüber externen Parteien wie Investoren, Analysten, Gesetzgebern, Regulierungsbehörden, Kunden und Mitarbeitern
- übernimmt gegenüber Mitarbeitern und der Gesellschaft Verantwortung
- ist auf Krisen und deren Bewältigung besser vorbereitet
- vergrößert die Sicherheit von unternehmens- und kundenspezifischen Informationen
- senkt das Risiko von Betrugsfällen

Über IT-Technologien lassen sich vermehrt Aspekte von GRC automatisieren und umsetzen. Auch hier hinterlässt die digitale Transformation ihre Spuren. Viele Unternehmen setzen deshalb IT-Komponenten ein, die für GRC genutzt werden.

Analystenfazit:

Mittels IT-Technologien lassen sich entscheidende Bereiche von *Governance*, *Risk Management* und *Compliance* automatisiert umsetzen. Das dient nicht nur der Erfüllung von Anforderungen, sondern hat einen praktischen Nutzen für die eigene Organisation.

5.2 Mit *Compliance* zum Geschäftserfolg

Regulatorische und geschäftliche Anforderungen stehen bei Anwendung von *GRC* nicht im Widerspruch zueinander, sondern beruhen auf gemeinsamen Intentionen. Es lassen sich überlappende Ziele zwischen äußeren Vorgaben und dem eigenen geschäftlichen Erfolg ableiten. Wenn etwa der Gesetzgeber von Informationsschutz spricht, spiegelt sich dies aus geschäftlicher Sicht im Schutz vor Betrug, Industriespionage oder im Wahren einer guten Reputation wider. Aus diesen Zielen lassen sich Kernbereiche ableiten, die Verantwortungsbereiche in Organisationen abbilden.

5.2.1 Nutzenpotenziale resultieren aus gemeinsamen Zielen

Vergleicht man die Absicht regulatorischer Vorgaben mit der Motivation geschäftlicher Anforderungen, so kristallisieren sich folgende gemeinsame Ziele heraus:

- **Schutz** von Informationen
- **Verfügbarkeit** von Informationen
- **Nachvollziehbarkeit** von Prozessen und der Verarbeitung von Informationen
- **Transparenz** gegenüber Dritten
- **Sorgfalt** im Geschäftsleben und
- die Unterstützung der **Dynamik** moderner Geschäftsprozesse, besonders im Hinblick auf die schnelllebigen Entwicklungen im Zuge der digitalen Transformation.



Abbildung 13: *Compliance*-Modell – Gemeinsame Ziele regulatorischer und geschäftlicher Anforderungen

Schutz von geistigem Eigentum, personenbezogenen Informationen, von Geschäftsstrategien sowie Finanz- und Vertriebsinformationen ist eine essenzielle Voraussetzung für das Fortbestehen und die Konkurrenzfähigkeit eines Unternehmens. Aus Sicht einer IT-basierten Verarbeitung dieser Informationen stellt die Gewährleistung von Vertraulichkeit und Integrität von Daten die grundlegenden Anforderungen dar. Diese Schutzaspekte finden sich in verschiedenen Regularien wieder:

- Bundesdatenschutzgesetz (BDSG, EU-DSGVO) und BDSAuditG
- GoBS
- Telekommunikationsgesetz (TKG)

- §§ 203 und 353b Strafgesetzbuch über den Umgang mit personenbezogenen Informationen
- zahlreiche Standards, die technische, organisatorische und Notfallmaßnahmen im Hinblick auf den Umgang mit Daten und Informationen festlegen, z. B. ISO27001/18, ISO 22301, Verschlusssachenanweisung (VS, VS-nfD), BSI-IT-Grundschutz oder der *Cloud Computing Compliance Controls Catalogue (C5)* des BSI

Verfügbarkeit stellt in einer weitgehend digitalisierten Arbeitswelt eine Grundvoraussetzung für das Funktionieren von geschäftskritischen Prozessen dar, sei es die Verfügbarkeit von Systemen, Diensten, Daten, Geräten oder Konnektivität. Ein weiterer Aspekt der Verfügbarkeit ist die Archivierung, also die mittel- bis langfristige Aufbewahrung von Informationen. Damit werden Unternehmen und Behörden vor Datenverlusten beim Ausfall von Systemen geschützt, und die Erfüllung gesetzlicher Vorgaben bezüglich des Zugriffs auf relevante Informationen wird gesichert. Dies umfasst etwa:

- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)
- Krankengeschichtenverordnung (KgVO)

In *Cloud*-Diensten wie beim *Outsourcing* wird eine definierte Leistungserbringung an Verfügbarkeit über **Service Level Agreements (SLAs)** garantiert. So kann die den regulatorischen und geschäftlichen Anforderungen entsprechende Sicherstellung der Verfügbarkeit an einen externen Dienstleister weitergereicht werden.

Nachvollziehbarkeit bezieht sich – in Abgrenzung zum externen Blickwinkel der Transparenz – auf die unternehmensinterne Sicht auf Abläufe und Strukturen. Sie umfasst Möglichkeiten der Prüfung und Auditierung von Geschäftsprozessen und Systemen sowie auch die kontinuierliche Verbesserung auf Basis der gewonnenen Erkenntnisse. Aus Unternehmenssicht ist von essenzieller Wichtigkeit, dass der Zugriff auf Informationen und deren Abruf jederzeit reproduzierbar sind, auch für forensische oder e-Discovery-Zwecke. Außerdem müssen den Geschäftsabläufen autorisierte Rollen zugeordnet und diese von entsprechend autorisierten Personen wahrgenommen werden. Auch beim Wissensmanagement in Unternehmen schafft ein hohes Maß an Nachvollziehbarkeit eine Struktur, die Genauigkeit und Konsistenz im Umgang mit Informationen und deren Lebenszyklus gewährleistet.

Transparenz bezieht sich auf externe Anforderungen in Bezug auf die Dokumentation von Geschäftsabläufen, die Orientierung an anerkannten Standards und die Einführung von Überwachungssystemen. Die Transparenzpflicht gegenüber externen Anspruchsgruppen kann auch unterstützend auf Geschäftsziele einwirken, wenn die Daten auch zur Optimierung verwendet werden. So können interne Entscheidungsprozesse verbessert und die Geschäftsagilität gesteigert werden. Darüber hinaus schafft Transparenz Vertrauen bei Kunden und Partnern und wirkt sich positiv auf die Reputation aus. Folgende Regularien gelten unter anderem in Bezug auf Transparenz:

- **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG):** Früherkennungssystem für potenzielle Risiken und Aussagen über Risiken und Risikostruktur eines Unternehmens
- **Handelsgesetzbuch (HGB):** Einhaltung von Vorschriften bei der Abschlussprüfung
- **Telekommunikationsgesetz (TKG):** Transparenzverpflichtung für Betreiber öffentlicher Telekommunikationsnetze, Offenlegung etwa von Informationen zur Buchführung oder technischen Spezifikationen

Sorgfalt ist ein entscheidender Faktor für die Sicherung der Wirtschaftlichkeit und Wirksamkeit der Geschäftstätigkeit eines Unternehmens. Dies umfasst die ausreichende Beschaffung von Informationen, eine adäquate Situationsanalyse und eine verantwortungsvolle Risikoeinschätzung, um zu fundierten und gesetzeskonformen Geschäftsentscheidungen zu kommen. Die Sorgfaltspflicht tangiert somit auch die Zielsetzungen der anderen Bereiche, Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz und Flexibilität.

Die einzelnen Sorgfaltspflichten sind überwiegend nicht schriftlich dokumentiert. Sorgfalt als Grundsatz der Unternehmensführung findet sich allerdings in einigen Regularien wieder, etwa im Aktiengesetz bzw. im GmbH-Gesetz, die beide die ordnungsgemäße Unternehmensführung unter Einhaltung von Gesetzen, Satzungen und Verpflichtungen beinhalten. Branchenspezifische Sorgfaltspflichten ergeben sich darüber hinaus aus den Anforderungen von Basel II oder dem Kreditwesengesetz (KWG) für das Finanzwesen. Diese umfassen Sorgfaltspflichten bezüglich wirksamer interner Kontrollen zur Vermeidung einer Kreditrisikokonzentration oder von Haftungsfällen. Aus Sicht der IT gehören insbesondere die Entwicklung und Etablierung von IT-Richtlinien dazu. Dabei sollten Branchenstandards und gesetzliche Vorgaben eingehalten und kontrolliert werden. Interne Trainings, Zertifizierungen und Audits können hierbei helfen.

Dynamik ist ein Ziel, das vor allem durch die Digitalisierung und Automatisierung von Geschäftsprozessen und *Workflows* entsteht. Dabei geht es um den Grad der Adaptierbarkeit bzw. Anpassbarkeit von *Compliance*-Anforderungen im Kontext von Digitalisierungsprojekten in einem Unternehmen oder einer Behörde. Aus Sicht neuer und alter regulatorischer Anforderungen ist Dynamik notwendig, um im Zuge der Transformation von Unternehmen die Erfüllung aller relevanten *Compliance*-Anforderungen zu gewährleisten. Aus geschäftlichem Blickwinkel führt die Dynamik zu einer höheren Zielerreichung hinsichtlich der anderen gemeinsamen Ziele: Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz und Sorgfalt. Darüber hinaus legt Dynamik den Grundstein dafür, dass interne Abläufe fortlaufend, effizient und flexibel an neue Technologien angepasst beziehungsweise Trends auch zeitnah agil und wirtschaftlich vertretbar zum Nutzen des Geschäftsziels umgesetzt werden können, ohne dabei die Einhaltung der *Compliance*-Vorgaben zu übergehen.

Analystenfazit:

Regulatorische und geschäftliche Anforderungen beruhen auf gemeinsamen Intentionen. Diese lassen sich über die sechs Ziele Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz, Sorgfalt und Dynamik formulieren und in die Tat umsetzen.

5.2.2 Kernbereiche regulatorischer und geschäftlicher Anforderungen

Nahezu alle regulatorischen und geschäftlichen Anforderungen haben einen Zusammenhang mit den genannten sechs gemeinsamen Zielen. Aus den Zielen lassen sich sechs Kernbereiche ableiten, auf die sich ein Unternehmen konzentrieren sollte, um den Anforderungen und Zielen erfolgreich gerecht zu werden. Diese Kernbereiche fallen in der Regel in jedem Unternehmen in die Verantwortung einer Person oder eines Bereichs. Es ist sinnvoll, die Aktivitäten unternehmensweit, also bereichs- und rollenübergreifend, wahrzunehmen, zu koordinieren und umzusetzen.

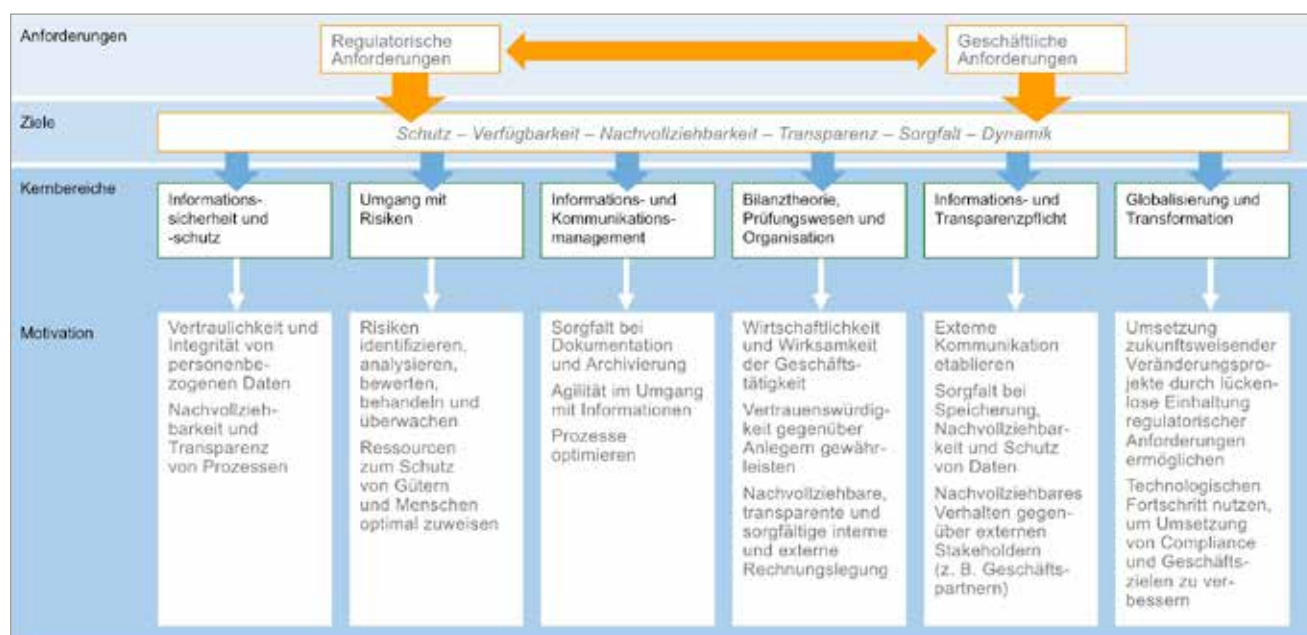


Abbildung 14: Compliance-Modell – Kernbereiche regulatorischer und geschäftlicher Anforderungen

Informationssicherheit und -schutz

Aus Unternehmenssicht sind Informationssicherheit und -schutz in mehrfacher Hinsicht wichtig. Dies betrifft vor allem Vertraulichkeit und Integrität von Informationen – bei kritischen und für das Fortbestehen des Unternehmens wichtigen Informationen, dem Schutz geistigen Eigentums, aber auch bei vom Gesetzgeber als schützenswert eingestuften Informationen.

Neben der Erfüllung juristischer Anforderungen sind Informationssicherheit und -schutz auch zur Nachvollziehbarkeit und Transparenz von Geschäftsprozessen notwendig, unter anderem im Sinne der Unveränderbarkeit von Protokollen. Datenabwanderungen aufgrund von unzureichenden Schutzmaßnahmen können sich zudem negativ auf die Reputation von Unternehmen auswirken.

Maßnahmen, um Informationssicherheit und -schutz zu gewährleisten, werden beispielsweise in den Standards COBIT (*Control Objectives for Information and Related Technology*), ITIL (*IT Infrastructure Library*), BSI-IT-Grundschutz, ISO 27001 sowie im IDW PS 330 des Instituts der Wirtschaftsprüfer in Deutschland e. V. (Prüfungsstandard) definiert.

USE CASES:

Die Contoso Glasmanufaktur GmbH betreibt einen Webshop, in dem Kundendaten mit personenbezogenen Informationen verarbeitet werden. Nach § 9 Datenschutzgesetz ist die Firma zur Ergreifung technischer und organisatorischer Sicherheitsmaßnahmen nach dem „Stand der Technik“ verpflichtet. Bei Verstößen gegen den Datenschutz sind Bußgelder und Reputationsverluste denkbar.

Man befürchtet bei Contoso hohe Kosten beim ständigen Ausbau des Webshops und dessen Anpassung an den Stand der Technik.

Lösung: Durch den Aufbau einer cloudbasierten Webshop-Lösung profitiert das Unternehmen von der Sicherheitsinfrastruktur des *Cloud*-Anbieters, die fortlaufend auf dem Stand der Technik gehalten wird. Eine eigene Zertifizierung des Shops ist nicht nötig, Lieferantenaudits müssen nicht oder nur in sehr beschränktem Umfang durchgeführt werden. Der *Cloud*-Anbieter verpflichtet sich zur Durchführung von Audits durch unabhängige Zertifizierungsstellen. Die Contoso Glasmanufaktur GmbH ist somit auch auf zukünftige Gesetzesänderungen vorbereitet.

Fazit: Mittels einer *Cloud*-Lösung kann der rasche technologische Wandel ohne eigenen größeren Aufwand mitgestaltet und vollzogen werden.

Am Contoso-Krankenhaus findet ein reger Informationsaustausch zwischen Patienten, Ärzten, der im Haus befindlichen Apotheke sowie externen Pflegediensten statt. Aufgrund zahlreicher Beschwerden wegen langer Wartezeiten sowie einiger Pannen mit den Pflegediensten sollen Kommunikation und Datenaustausch verbessert werden.

Über eine webbasierte Plattform können Patienten Termine vereinbaren sowie Medikamente und Überweisungen zu externen Ärzten anfordern.

Lösung: Da sehr unterschiedliche Personengruppen über das Portal auf Daten zugreifen, ergeben sich für das Identitäts- und Zugriffsmanagement besondere Herausforderungen. Deshalb wurden Programmierung und Betrieb des Portals an einen zertifizierten Anbieter vergeben. Im Portal ist eine strikte Trennung der Daten der unterschiedlichen Personengruppen vorgesehen. Daten werden zwischen den Personengruppen über Software-Agenten transportiert, die die Berechtigungen jedes einzelnen Zugriffs prüfen.

Fazit: Für ein komplexes Identitäts- und Zugriffsmanagement bietet sich eine zentralisierte Lösung mit strengen Kontrollen aller Zugriffe an.

Umgang mit Risiken

Der Umgang mit Risiken ist ein systematischer Ansatz und Prozess zur Identifikation, Analyse Bewertung, Behandlung und Überwachung von Risiken (siehe GRC). Damit erkennen Unternehmen Bedrohungen, Schwachstellen und letztlich Risiken für das eigene Geschäftsmodell. Risiken werden so weit wie möglich kalkuliert, die Höhe der Risikoakzeptanz festgelegt und Prioritäten bei angepassten Maßnahmen gesetzt. Das rechtfertigt auch Investitionen in Sicherheitsmaßnahmen und führt letztlich zu einem höheren Sicherheitsbewusstsein im Unternehmen – auch und insbesondere beim Management. Eine wichtige Motivation beim Umgang mit Risiken liegt in der Verbesserung der Zuweisung von Ressourcen zum Umgang mit Bedrohungen und der Reduktion des Risikos auf ein akzeptables Maß.

Die generischen Ziele beim Umgang mit Risiken liegen im Schutz und der Verfügbarkeit von Daten, der Nachvollziehbarkeit von Prozessen und dem Erfüllen der Sorgfaltspflicht insgesamt. Zwar ist der Umgang mit Risiken Gegenstand zahlreicher Regularien und Standards, etwa dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), Basel III und COBIT. Nichtsdestotrotz liegen die Nutzenpotenziale aus geschäftlicher Sicht auf der Hand: Ein systematischer Ansatz zum Umgang mit Risiken ist notwendig, um Risiken korrekt einzuschätzen und entsprechende Maßnahmen zur Vermeidung von Verlusten zu ergreifen.

USE CASES:

Bei der Contoso Financial Service GmbH gibt es ein IT-gestütztes Risikowesen. Parallel dazu gibt es ein zweites, auf Excel-Tabellen basierendes System zur Erfassung von *Compliance*-Anforderungen und -Risiken.

Es ist geplant, die beiden Systeme zusammenzufassen, damit ein transparenter Überblick über alle Risiken möglich ist. Bei der Umsetzung gibt es Schwierigkeiten technischer und organisatorischer Natur.

Lösung: Das gesamte Risikowesen wird in die *Cloud* an einen externen Dienstleister verlagert. Mitarbeiter und Führungskräfte können sich über ein *Web Interface* mit den benötigten Informationen versorgen.

Fazit: Statt der aufwendigen Integration unterschiedlicher Dienste bieten sich oftmals *Cloud*-Lösungen an, die interne Ressourcen schonen.

Die Contoso Industrial AG besitzt ein proprietäres CRM-System zur Verwaltung von Kundenbeziehungen. Dieses wird *in-house* betrieben, wobei Lizenzgebühren pro Device mit Zugriff auf das System entstehen. Die Lizenzakquise wird nebenher von der IT-Abteilung durchgeführt. Es gibt allerdings kein zentrales und transparentes Lizenzmanagement.

Aufgrund des schnellen Wachstums der Firma werden zahlreiche neue Mitarbeiter mit ihren Devices an das System angebunden. Die Gefahr von Lizenzüber- bzw. -unterdeckung steht im Raum – es bestehen die Risiken unnötiger Kosten oder von Lizenzverletzungen.

Lösung: Nach der Adaption eines cloudbasierten CRM-Systems im *SaaS*-Modell wird nun jeder Zugriff, Account sowie die Ressourcennutzung klar dokumentiert und bepreist (Transparenz). Das Lizenzmanagement auf Kundenseite entfällt.

Fazit: Die Gefahr von Lizenzverletzungen oder Überdeckung wird mit einem *Cloud*-Dienst gebannt.

Informations- und Kommunikationsmanagement

Im Rahmen des Informations- und Kommunikationsmanagements erfolgt das Planen, Gestalten, Überwachen und Steuern von Informationsflüssen. Für diese Aktivitäten werden nachvollziehbare und reproduzierbare Geschäftsprozesse benötigt, die auf einer sicheren und effizienten IT-Infrastruktur aufbauen.

Trotz permanenten Datenwachstums und zunehmender Flexibilisierung von Geschäftsprozessen müssen Unternehmen spezifische Informationen bei Bedarf schnell finden und abrufen. Dies fordern beispielsweise die GoBD und die Regelungen des Bilanzrechtsmodernisierungsgesetzes (BilMoG). Weitere rechtliche Regelungen, welche die Aufbewahrung von Daten betreffen, lassen sich im Bereich der Produkthaftung und der Prozessordnung finden. Beim Umsetzen dieser Forderungen hilft etwa der standardisierte *ITIL*-Prozess.

Über das Informations- und Kommunikationsmanagement erreichen Unternehmen auch strategische Ziele durch methodische Informationssteuerung und Kommunikation. Um diese effektiv anzuwenden, ist es unumgänglich, bei Dokumentation und Archivierung mit angemessener Sorgfalt vorzugehen. Die Schnittmenge zwischen geschäftlichen und regulatorischen Anforderungen liegt hier also insbesondere im Erreichen von Verfügbarkeit, Nachvollziehbarkeit und letztlich der Sorgfaltspflicht im Informationslebenszyklus. Dabei ist ein Lösungsansatz zur Klassifizierung von Daten nötig, um Informationen gemäß den rechtlichen und unternehmensinternen Anforderungen differenziert zu verwalten.

USE CASES:

Bei der Stadtverwaltung von Contoso City ergeben sich für die Einwohner unzumutbare Wartezeiten bei Routinearbeiten wie etwa der Ausstellung von Parkausweisen, An- und Abmeldung von Hunden, der Verlängerung von Personalausweisen und Reisepässen sowie bei der Auskunft des aktuellen Status von Anfragen.

Die hinter den diversen Verwaltungsakten stehenden Geschäftsprozesse sollen durch eine einheitliche Infrastruktur unterstützt werden und soweit wie möglich in automatisierte *Workflows* übertragen werden.

Lösung: Die Einwohner von Contoso City erhalten über ein *Web Interface* Zugang zu einem cloudbasierten Portal, über das sie die verschiedenen Verwaltungsakte anstoßen und den jeweiligen Bearbeitungsstatus einsehen können. Bei Verwaltungsakten ohne größeren Sicherheitsbedarf (Parkausweis, Hundesteuer) geschieht die Anmeldung am Portal über Benutzername und Passwort. Andere Funktionen des Portals können mit Hilfe des elektronischen Personalausweises aktiviert werden.

Fazit: Geschäftsprozesse und ihre *Workflows* können in ihren funktionalen Abläufen unter Berücksichtigung des Schutzbedarfs der Daten modelliert und gehandhabt werden. Damit werden die Geschäftsprozesse transparenter und schneller – überflüssige Wartezeiten entfallen.

Die Contoso Industrial AG ist in den letzten Jahren stark gewachsen. Auch die Anzahl von Mitarbeitern hat sich stetig erhöht. Bei Problemen mit der IT melden sich die Mitarbeiter bei dem zentralen *Service Helpdesk* der Firma. Dort werden die Probleme in Form von Tickets aufgenommen und bearbeitet. Bisher wurden die Tickets manuell erfasst und bearbeitet. Diese manuelle Bearbeitung von Tickets ist an ihre Kapazitätsgrenze gekommen, sodass die Anfragen verzögert beantwortet werden.

Es soll ein schneller und sauber definierter Prozess zur Ticketverarbeitung auch bei hoher Belastung durch viele Tickets bzw. Anfragen implementiert werden

Lösung: Der *Workflow*, der zur Erstellung und Bearbeitung von Tickets benötigt wird, wird in einer *Cloud*-Lösung gehostet und weitgehend automatisiert. Routineanfragen werden über ein webbasiertes *Self-Service*-Portal erfasst. Die automatische Ticketverarbeitung wendet klare Regeln bei der Weiterleitung von Tickets an Vorgesetzte an.

Fazit: Mobile Erreichbarkeit und Skalierbarkeit aus der *Cloud* schaffen hohe Nachvollziehbarkeit von Fehlerfällen, erhöhen Reaktionsfähigkeit und reduzieren den Verbrauch von Ressourcen.

Bilanztheorie, Prüfungswesen und Organisation

Dieser Kernbereich umfasst mit der Bilanztheorie die Bewertung der Vermögensgegenstände eines Unternehmens sowie die von diesem erzielten Erträge. Damit werden *Compliance*-Vorgaben aus dem Steuer- und Handelsrecht umgesetzt. Das Prüfungswesen überwacht Effizienz und Effektivität bei der Umsetzung der Kernelemente und dient der Sicherung von Wirtschaftlichkeit und Wirksamkeit der Geschäftstätigkeit eines Unternehmens.

Dieser Kernbereich ist zudem notwendig, um Nachvollziehbarkeit, Transparenz und Sorgfalt der internen und externen Rechnungslegung sowie die Einhaltung der maßgeblichen rechtlichen Vorgaben zu garantieren. Dies erfolgt in der Regel durch ein internes Steuerungs- und Überwachungssystem, ergänzt durch ein Risikomanagement.

Die Notwendigkeit dieser gesetzlichen Forderungen entsteht durch länderspezifische Prüfungsstandards, wie etwa dem IDW PS 330 – Abschlussprüfung bei Einsatz von Informationstechnologie. Diese haben für einen Abschlussprüfer rechtliche Bindung und müssen somit vom Unternehmen indirekt befolgt werden.

USE CASES:

Die Contoso Industrial AG ist als börsennotiertes Unternehmen nach § 37 Wertpapierhandelsgesetz dazu verpflichtet, regelmäßig Finanzberichte zu erstellen. Diese müssen im Internet veröffentlicht sowie im Unternehmensregister gespeichert werden. Zudem sind Hinweisbekanntmachungen an verschiedene Empfänger nötig.

Hinweisbekanntmachungen und Veröffentlichung der Finanzberichte wurden bisher manuell durchgeführt. Es soll ein System eingerichtet werden, das diese Tätigkeiten automatisch abwickelt.

Lösung: Die mit Hinweisbekanntmachungen und Veröffentlichung zusammenhängenden *Workflows* wurden analysiert und mittels einer Software automatisiert. Damit muss nur noch eine Liste mit Adressaten gepflegt werden. Der Versand von Hinweisen und Berichten sowie das Einspeisen in die Homepage der Contoso Industrial AG erfolgen automatisch.

Fazit: Die Automatisierung von *Workflows* befreit Mitarbeiter von Routinearbeiten.

Die Contoso Glasmanufaktur GmbH betreibt einige regionale Läden sowie einen Internet-Versandhandel. Die Geschäftsleitung möchte die bisher größtenteils analoge Finanzberichterstattung und Archivierung digitalisieren. Dabei müssen alle handels- und steuerrechtlichen Grundsätze beachtet werden.

Mit dem Einsatz von IT sollen die Archivierungspflichten nachhaltig umgesetzt werden, also auch im Hinblick auf neu entstehende Anforderungen. Eine Kostenschätzung zeigt, dass Identifikation, Umsetzung und Kontrolle entsprechender Maßnahmen (z. B. Zertifizierung) sehr kostenintensiv wären.

Lösung: Eine *Cloud*-Lösung zur Archivierung und Finanzberichterstattung ermöglicht die Nutzung von Diensten, welche die Anforderungen erfüllen und bei denen die notwendigen Audits und Zertifizierungen durchgeführt werden.

Fazit: Das Unternehmen bleibt flexibel und erreicht trotzdem eine Ausrichtung der IT-Prozesse an gängige Standards.

Transparenz- und Informationspflicht

Die Informations- und Transparenzpflicht eines Unternehmens hängt eng mit Datenschutz, Informations- und Risikomanagement sowie internen Kontrollsystemen zusammen. Zu ihren Voraussetzungen zählen entsprechend verfügbare Daten, die nachvollziehbar und transparent sind und mit Sorgfalt erhoben und gepflegt wurden.

Die Informations- und Transparenzpflicht ist sowohl ereignisgetrieben als auch ein kontinuierlicher Prozess. Ersteres trifft beispielsweise auf das Bundesdatenschutzgesetz und die dort festgehaltenen Betroffenenrechte bei Datenschutzverletzungen zu. Die Richtlinie 2004/39/EG über Märkte für Finanzinstrumente (MiFID), die Geschäftsprozesse für den Lieferantenwechsel im Gassektor (GeLi Gas) und die GoBD sind weitere Beispiele für die Informations- und Transparenzpflicht. Auch das IT-Sicherheitsgesetz setzt hier Akzente, etwa bei der für Telekommunikationsunternehmen verpflichtenden Warnung von Kunden bei einem Missbrauch eines Kundenanschlusses.

Auch wenn viele Unternehmen die Informations- und Transparenzpflicht als unangenehm empfinden, ermöglicht sie auch Synergien in Bezug auf geschäftliche Ziele. Hierzu gehört die externe Kommunikation, optimierte Prozesse, die Pflege und Wahrung der eigenen Reputation, der verantwortungsbewusste Umgang mit Daten und vor allem die Einführung eines Kontrollsystems, das kritische Ereignisse zeitnah erkennt und eine adäquate Reaktion anfordert und überwacht.

USE CASES:

Die Contoso Financial Service GmbH ist nach dem Geldwäschegesetz verpflichtet, gegen Geldwäscheaktivitäten auf Bankkonten vorzugehen und die Behörden bei der Aufklärung zu unterstützen.

Lösung: *Big Data Analytics* aus der *Cloud* zur Identifikation verdächtiger Aktivitäten erhöht die Transparenz der Bank und spart Ressourcen. So kann unter Bindung weniger Mitarbeiter eine höhere *Compliance* erreicht werden.

Fazit: *Big Data Analytics* ist ein Werkzeug, um *Compliance*-Anforderungen bei großen Datenmengen umzusetzen.

Die Contoso Industrial AG hat in den letzten Jahren zahlreiche Firmen im Ausland hinzugekauft und ist so zu einem internationalen Konzern geworden. Die Tochterfirmen sollen in den Mutterkonzern integriert werden. Aufgrund des schnellen Wachstums ist der Überblick verloren gegangen, welche regulatorischen *Compliance*-Anforderungen für die jeweiligen Töchter existieren und wer Kenntnis von den jeweiligen Anforderungen haben muss.

Lösung: Jede Tochtergesellschaft erfasst die für sie geltenden Anforderungen und Verantwortlichkeiten in einem zentralen, webbasierten System. Die Anforderungen lassen sich anschließend transparent abrufen und kommunizieren.

Fazit: Die Schaffung von *Awareness* ist stets mit Transparenz und Kommunikation verbunden. IT-Systeme bieten dazu eine wertvolle Unterstützung.

Globalisierung und Transformation

Dieser letzte Kernbereich widmet sich der steigenden Dynamik, welche Unternehmen im Zuge der digitalen Transformation vor schnelllebige technologische und organisatorische Veränderungen stellt. Geschäftsprozesse fußen – wie erläutert – immer stärker auf der IT. Auch Unternehmensbereiche, die bisher vornehmlich durch analoge *Workflows* geprägt waren, greifen immer stärker auf innovative IT-Technologien zurück. Die *Cloud* steht dabei im Zentrum dieser Entwicklung als Garant für die mobile Verfügbarkeit und die Vereinheitlichung von Datenflüssen über technologische, organisatorische und Landesgrenzen hinweg. Um dieses Potenzial abzurufen, müssen Unternehmen und Behörden ein hohes Maß an Flexibilität im Umgang mit Technologien und im Hinblick auf die eigene Organisationsstruktur an den Tag legen.

Der *Compliance* kommt im Kontext der digitalen Transformation auch deshalb eine Schlüssel-funktion zu, weil die Erfüllung regulatorischer Anforderungen eine Voraussetzung für die Adaption von Technologien und Veränderungen im Allgemeinen ist. *Compliance*-Anforderungen, die sich aus Veränderungen ergeben, müssen in allen Unternehmensbereichen bekannt und umgesetzt sein. Wer das Thema *Compliance* im Hinblick auf Veränderungen also frühzeitig angeht, verbessert seine Chancen auf Effizienzsteigerungen und Wettbewerbsvorteile durch Innovation und erhöht somit auch seinen Geschäftserfolg.

USE CASES:

Die Contoso Industrial AG verändert ihre Organisationsstruktur. Dabei stellt sich die Frage, ob alle *Compliance*-Anforderungen noch erfüllt werden. Zwar werden Teilbereiche regelmäßig über Audits abgeprüft, allerdings entsteht dabei kein organisationsweites, umfassendes Bild über die *Compliance*.

Lösung: Mit Hilfe eines IT-Systems werden zentrale Kernbereiche der *Compliance*-Anforderungen identifiziert, und ein regelmäßiges, unternehmensweites *Assessment* wird organisiert. Dabei werden im System Ansprechpartner für jeden Bereich hinterlegt.

Fazit: Bei zukünftigen Änderungen an der Organisationsstruktur können Transparenz über den eigenen *Compliance*-Status hergestellt und Handlungsfelder zum schnellen Ergreifen von Maßnahmen abgeleitet werden.

Die Stadtverwaltung von Contoso City hat ihre IT schon vor Jahren in eine eigene Firma ausgelagert und nutzt deren Dienste als *Managed Service* und aktuell verstärkt für *Cloud*-Lösungen. Der Erfolg des Bürgerportals hat dazu geführt, dass die Verwaltung immer neue Projekte für die Transformation von *Workflows* in *Cloud*-Applikationen ins Leben ruft.

Die Verwaltungsleitung benötigt Informationen, um Nutzen und Sicherheit der angedachten *Cloud*-Lösungen zu bewerten. Für die Umsetzung aller Ideen ist nicht genügend Budget vorhanden.

Lösung: Mittels einer IT-Lösung werden die diversen *Workflows* erfasst und nach verschiedenen Kriterien wie Aufwand, mögliche Kostenersparnis, Sicherheit und den Nutzen durch beschleunigte *Workflows* bewertet. Die Leitung kann nun entscheiden, welche Projekte umgesetzt werden.

Fazit: Die digitale Transformation ist kein Selbstzweck. Mit Hilfe der IT kann der Nutzen der Digitalisierung bewertet werden.



Analystenfazit:

Die für regulatorische und geschäftliche Anforderungen wesentlichen sechs Ziele lassen sich durch Aktivitäten in sechs Kernbereichen abbilden. Diese Aktivitäten dienen der Erfüllung externer Vorgaben, steigern aber gleichzeitig das Potenzial für den eigenen Geschäftserfolg.

KAPITEL 6

53

ANWENDUNG DES *COMPLIANCE*-MODELLS

6. ANWENDUNG DES COMPLIANCE-MODELLS

Bisher wurde das *Compliance*-Modell in erster Linie als Verständnismodell beschrieben, das potenzielle Synergien in Zielen und Kernbereichen strukturiert abbildet. In diesem Kapitel werden nun Brücken ins operative Geschäft geschlagen und Ansätze zur konkreten Nutzung des Modells diskutiert. In Abschnitt 6.1 werden zu diesem Zweck Handlungsfelder als weitere Komponenten des Modells eingeführt, die zentrale Tätigkeiten und Zuständigkeiten in einer Organisation abbilden und kategorisieren. In Abschnitt 6.2 werden für jeden Kernbereich beispielhafte Handlungsfelder beschrieben. Die Grundlage für die Erreichung der gemeinsamen Ziele des Modells sind zentrale Prozesse, mit denen *Compliance*-Anforderungen ermittelt und umgesetzt werden. Es gilt also, das Rahmenwerk des Modells zu nutzen, um relevante Prozesse im eigenen Unternehmen zu erkennen, zu evaluieren und ggf. zu verändern. In Abschnitt 6.3 werden hierzu zwei unterschiedliche Ansätze dargestellt.

6.1 Vom Verständnis- zum Anwendungsmodell

Im vorherigen Kapitel wurde ein Verständnismodell eingeführt, das die Anforderungen regulatorischer und geschäftlicher Ziele in sechs Kernbereichen abbildet. Das ist ein notwendiger Schritt, um einen vereinheitlichten Umgang und eine gemeinsame Sprache in Bezug auf die komplexe Thematik zu entwickeln. Unternehmen, die sich bereichsunabhängig und systematisch mit den Kernbereichen auseinandersetzen, erlangen über das Modell nicht nur Kenntnis über die wesentlichen regulatorischen Anforderungen, sondern auch über konkrete Handlungsfelder, in denen Synergien zwischen *Compliance* und Geschäftserfolg erzielt werden können.

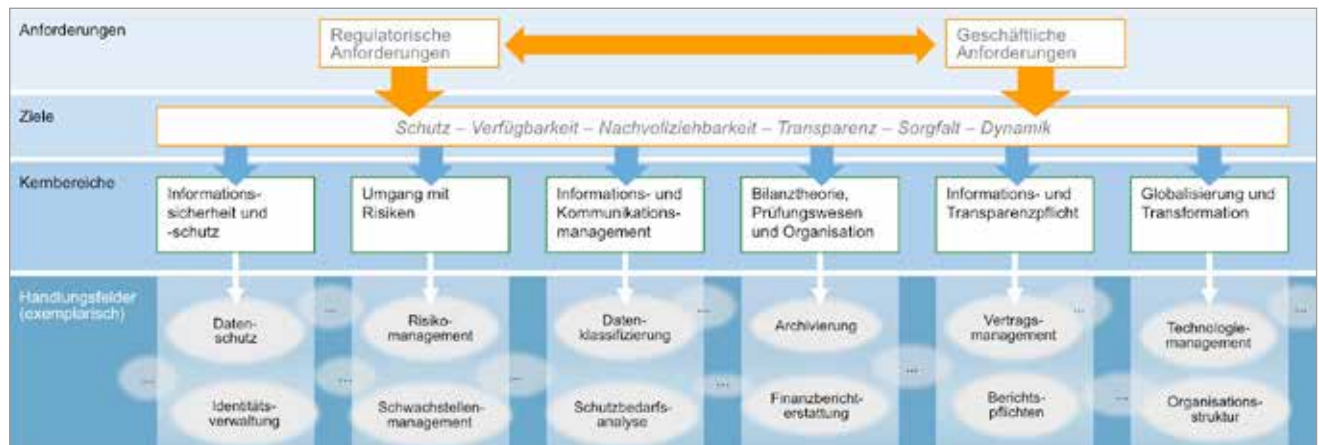
6.1.1 Verfeinerung des Modells

Wie kann eine solche Auseinandersetzung effektiv und im Kontext einer bestehenden Prozesslandschaft stattfinden und wie können passende Maßnahmen für das eigene Unternehmen getroffen werden? Die Lösung liegt in der Identifikation von Handlungsfeldern, mit denen das Modell verfeinert wird und die konkreten Notwendigkeiten für die Einhaltung von Anforderungen beschreiben. Auf Basis solcher Handlungsfelder können Prozesse definiert werden, die einen Beitrag zur unternehmensweiten Umsetzung der Anforderungen der Kernbereiche leisten.

Die zur Ermittlung von Handlungsfeldern benötigten zentralen Prozesse müssen Maßnahmen definieren, die es trotz rascher organisatorischer und technologischer Veränderungen ermöglichen, alle *Compliance*-Anforderungen zu erfüllen, und zwar vor, während und nach Veränderungen. So wird verhindert, dass Änderungen an Geschäftsprozessen zu Einbrüchen bei der *Compliance* führen, und seien diese auch nur temporär. Ein Unternehmen kann Handlungsfelder bestimmen, indem es einen kritischen Abgleich der eigenen Prozesslandschaft mit den Anforderungen der Kernbereiche durchführt. Jedem Kernbereich werden Handlungsfelder zugeordnet, aus denen sich konkrete Verbesserungsmaßnahmen für die jeweils relevanten Prozesse generieren lassen. Gegebenenfalls kann sogar die Notwendigkeit der Etablierung eines neuen Prozesses aus der Bestimmung eines oder mehrerer Handlungsfelder erwachsen. Es empfiehlt sich, eine zentrale, prozessübergreifende Steuerung der Handlungsfelder zu etablieren, um Synergien zu erreichen und damit potenziell multiplizierten Aufwand zu reduzieren. Die zentrale Organisation der Nutzung von Maßnahmen und Kontrollen ermöglicht die Identifizierung von wiederholbaren Einsatzmöglichkeiten, eben für die Erfüllung von *Compliance*-Anforderungen und die Unterstützung von betriebswirtschaftlichen Geschäftszielen.

6.1.2 Analyse als Basis für unternehmerisches Handeln

Das *Compliance*-Modell dient also nicht nur als **Verständnismodell**, sondern ist als **Anwendungsmodell** ein Rahmenwerk für die Bewertung der eigenen Prozesslandschaft und die Bestimmung potenzieller Verbesserungen. Um dies konkret darzustellen, wird das Modell in der folgenden Abbildung um je zwei exemplarische Handlungsfelder erweitert.



Compliance-Modell – Exemplarische Handlungsfelder

Während die Kernbereiche regulatorischer und geschäftlicher Anforderungen also im Groben reglementierte Aspekte der IT-Nutzung umfassen, stellen die den Kernbereichen zugeordneten Handlungsfelder konkrete Ansätze und Bereiche unternehmerischen Handelns zur Umsetzung der Ziele dar. Die Handlungsfelder müssen dabei durch Prozesse und *Workflows* umgesetzt werden.

Ein Unternehmen, das sich umfassend und bereichsübergreifend mit der Analyse der eigenen Prozesslandschaft auseinandersetzt, erhält auf diese Weise einen Überblick über all jene Bereiche, in denen die Erreichung regulatorischer und geschäftlicher Ziele notwendig ist und gegebenenfalls verbessert werden kann. Die Gestaltung bzw. Verbesserung der *Compliance*-Prozesse kann dann basierend auf den individuell bestimmten Handlungsfeldern unternehmensweit durchgeführt werden, wobei auch eine Wiederverwendung von Maßnahmen möglich ist.

Analystenfazit:

Das *Compliance*-Modell ist dreistufig aufgebaut. Aus allgemeinen Zielen ergeben sich Kernbereiche von Aktivitäten, die schließlich über Prozesse und *Workflows* in bestimmten Handlungsfeldern umgesetzt werden.

6.2 Handlungsfelder zur Verbesserung des Geschäftserfolges

Nachdem im vorherigen Abschnitt der strategische Nutzen von Handlungsfeldern beschrieben wurde, stellt sich nun die Frage, welche konkreten Zielsetzungen mit Hilfe der Handlungsfelder abgedeckt werden können. Im folgenden Abschnitt findet eine detaillierte Auseinandersetzung mit je einem Handlungsfeld pro Kernbereich statt. Zwar deckt diese Darstellung nur einen sehr kleinen Teil aus der großen Menge möglicher Handlungsfelder für Organisationen und Unternehmen ab. Dennoch machen die Beispiele deutlich, dass die Verbesserung von Prozessen, welche auf die Einhaltung regulatorischer Anforderungen abzielen, auch für den Geschäftserfolg Nutzen bringt.

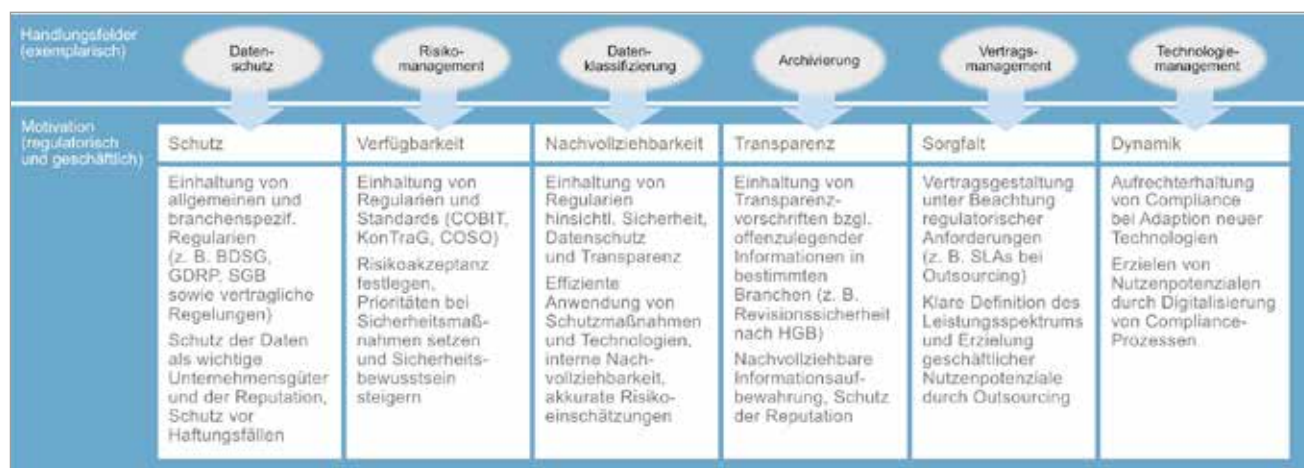


Abbildung 15: Compliance-Modell – Motivation exemplarischer Handlungsfelder

6.2.1 Informationssicherheit und -schutz

Beim Thema Informationssicherheit und -schutz greifen Handlungen mehrerer Kernbereiche ineinander. Zur Festlegung sinnvoller IT-Sicherheits- und Datenschutzrichtlinien sowie zum Management von Identitäten und Zugriffsrechten muss die Klassifizierung von Daten nach ihrem Schutzbedarf umgesetzt werden, etwa hinsichtlich branchen- und eigentümer-spezifischer Anforderungen. Auch die Identifikation und Bewertung von Risiken spielt in diesem Kontext eine wichtige Rolle, um Schutzbedarfe festzustellen und Maßnahmen zu motivieren.

Im Allgemeinen muss die IT-Landschaft einer Organisation im Hinblick auf logische und physische Schwachstellen überwacht werden. Zudem ist ein sauber definierter Prozess für den Umgang mit Vorfällen und Sicherheitsverletzungen erforderlich. Die Handlungen konzentrieren sich auf die Einhaltung spezifischer Regularien (z. B. Datenschutz). Gleichzeitig leisten Maßnahmen der Informationssicherheit einen entscheidenden Beitrag zum Schutz wichtiger Unternehmensgüter sowie der Reputation und beugen Haftungsfällen durch Nichteinhaltung vor.

Die beiden exemplarischen Handlungsfelder **Datenschutz** und **Identitätsverwaltung** werden im Folgenden weiter konkretisiert:

Das Handlungsfeld **Datenschutz** umfasst alle Prozesse und Maßnahmen zur Umsetzung regulatorischer Anforderungen zum Schutz sensibler Daten. Sensible Daten enthalten beispielsweise personenbezogene (Kunden-)Informationen. Auch und gerade infolge der zunehmenden Automatisierung der Datenverarbeitung muss der Schutz solcher Daten vor unbefugten Zugriffen sichergestellt werden, um gesetzlichen und ggf. auch branchenspezifischen Anforderungen zu genügen. Unternehmen müssen relevante Datenschutzvorgaben identifizieren, umsetzen und die Einhaltung fortlaufend überprüfen. Änderungsprozesse an Richtlinien und Prozessen müssen wahrgenommen und hinsichtlich möglicher Auswirkungen auf die eigenen Prozesse evaluiert werden. Gegebenenfalls können so notwendige Anpassungen in Prozessen, der Organisation und der IT-Infrastruktur frühzeitig umgesetzt werden.

Im Handlungsfeld **Identitätsverwaltung** wird ein Sicherheitskonzept angestrebt, welches die große Anzahl an Benutzern, Systemen, Daten und anderen IT-Ressourcen umfasst, Zugriffsmöglichkeiten auf Ressourcen auf ein notwendiges Minimum reduziert und Aktivitäten und Zugriffsversuche nachvollziehbar macht. Hierzu ist ein einheitlicher und dokumentierter Prozess erforderlich, der Identitäten sowie die Zugriffe auf relevante Systeme und Kommunikationskanäle verwaltet und überwacht. In vielen Systemen hat sich das Modell der rollenbasierten Zugriffskontrolle (RBAC) durchgesetzt, welches Benutzerrechte auf Basis einer den Benutzern zugeordneten Rolle sowie Gruppen vergibt.

6.2.2 Umgang mit *IT-Compliance*-Risiken

Grundsätzlich stehen im Umgang mit Risiken vier Ansätze zur Auswahl.

- Eine häufige Vorgehensweise ist das Reduzieren von Risiken durch geeignete **technische und organisatorische Maßnahmen (TOM)** sowie Kontrollmechanismen.
- Zweitens lassen sich Risiken zum Teil auf **externe Parteien übertragen**, z. B. auf Versicherungen oder (mit Einschränkungen) auf Dienstleister.
- Das Vermeiden von Risiken durch **Einstellung von Aktivitäten**, die zu Risiken führen, z. B. durch Re-Design von Geschäftsprozessen oder Vermeidung neuer, unsicherer IT-Systeme, ist eine weitere Option.
- Zu guter Letzt besteht die Möglichkeit, **Risiken zu akzeptieren**, wenn die Gegenmaßnahmen in keinem Verhältnis zum Wert des Geschäftsgutes stehen. Wichtige Handlungsfelder im Umgang mit Risiken stellen unter anderem das **Risikomanagement** und das **Schwachstellenmanagement** dar.

Egal, für welchen Ansatz man sich entscheidet – für die Umsetzung ist in jedem Fall ein klar geregeltes **Risikomanagement** erforderlich, welches Maßnahmen zur Erkennung, Analyse und Überwachung sowie Kriterien zur Bewertung von Risiken in Bezug auf konkrete Güter festlegt und die individuellen Rahmenbedingungen der getroffenen Entscheidung dokumentiert. Bei der Identifikation und Bewertung von Risiken werden alle im Unternehmen vorhandenen Güter, also etwa Systeme, Informationen, Produktionsanlagen etc., berücksichtigt. Wichtig ist auch die Definition von Rollen im Risikomanagement sowohl auf übergeordneter Ebene als auch im IT-Risikomanagement. Unternehmensweite Abstimmungsprozesse zwischen den Beteiligten sind ebenso zu etablieren, wie die Ausrichtung auf ein gemeinsames unternehmensweites Risikomanagementrahmenwerk. Hierzu zählen Bewertungsverfahren für Risiken und die Integration von Risiken unterschiedlicher Bereiche, etwa IT-, Vertrags- und Unternehmens-Risiken, in ein einheitliches Konzernrisikowesen.

Expertenstatement: *Compliance*-Risiken werden gesenkt durch Schaffung von übergreifenden Standards und Reduzierung der Komplexität. Darüber hinaus sind Regelungen und die Durchsetzung klarer Verantwortlichkeiten nötig.

Dem **Schwachstellenmanagement** kommt speziell beim Management von IT-Risiken eine wichtige Rolle zu, da auf diese Weise die aktuelle Bedrohungslage für wichtige digitale Unternehmensgüter bestimmt wird und entsprechende Gegenmaßnahmen ergriffen werden können. Sollten kritische Informationen durch Schwachstellen bedroht sein, so wird das betroffene Unternehmen schnellstmöglich die Behebung der Schwachstelle, beispielsweise durch Updates oder neue Sicherheitsmaßnahmen, veranlassen. Hier zeigt sich auch die Bedeutung des Umgangs mit Risiken für andere Kernbereiche – in diesem Fall der Informationssicherheit und des -schutzes.

6.2.3 Informations- und Kommunikationsmanagement

Die Gestaltung von Geschäftsprozessen und Infrastrukturen, die den Umgang mit Informationen beeinflussen und steuern, ist für verschiedene Unternehmensbereiche und -funktionen von zentraler Bedeutung. Das Informations- und Kommunikationsmanagement ermöglicht die Verarbeitung und Haltung von Daten auf Basis einer zentralen und einheitlichen Infrastruktur und schafft somit die Grundlage für die Steuerung von Datenhaltung und Kommunikation nach rechtlichen und geschäftlichen Vorgaben. Auf Anwendungsebene stehen vor allem *Enterprise Content Management (ECM)* und Geschäftsprozess-Management (BPM) als Querschnittsdisziplin im Fokus. *Enterprise Resource Planning (ERP)* und *Business Intelligence (BI)* sind weitere Applikationen, die das Informations- und Kommunikationsmanagement berühren.

Handlungsfelder, die sich aus dem Informations- und Kommunikationsmanagement herleiten, sind beispielsweise die **Klassifizierung** und die **Bestimmung des Schutzbedarfs von Daten**. Diese beiden Handlungsfelder hängen stark voneinander ab und werden mit der Unterstützung technischer Analyseverfahren und unternehmensweit einheitlicher Prozesse, Kriterien und Regeln bearbeitet. Beide Handlungsfelder sorgen für die Erfüllung von Sicherheits-, Datenschutz- und Transparenzanforderungen und führen zu einer effizienteren Zuweisung von Schutzmaßnahmen, einer besseren Einschätzung und Nachvollziehbarkeit des Schutzbedarfs unterschiedlicher Datenarten und infolgedessen zu genaueren Risikoeinschätzungen.

6.2.4 Bilanztheorie, Prüfungswesen und Organisation

Das Bilanz- und Prüfungswesen beschäftigt sich im weitesten Sinne mit der Umsetzung regulatorischer Anforderungen aus dem Steuer- und Handelsrecht über länder- und branchenspezifische Standards. Unternehmen richten ihre Prozesse an gemeinsamen Standards aus (beispielsweise COSO) und etablieren ein internes Kontrollsystem (IKS) zur Steuerung und Überwachung. Hierbei gelten in der Regel vier Prinzipien:

- Das **Prinzip der vier Augen** erfordert eine gegenseitige Kontrolle jedes *Workflows* durch einen anderen Mitarbeiter, sodass für jeden kritischen Prozess mindestens zwei Mitarbeiter verantwortlich sind.
- Das **Prinzip der Funktionstrennung** („*segregation of duties*“) sorgt für die Trennung zwischen Auftragserfüllung und Auftragskontrolle.
- Das **Prinzip der Transparenz** besagt, dass Konzepte für Unternehmensprozesse nachvollziehbar und verständlich sein müssen. Über Kontrollziele kann objektiv und von Außenstehenden geprüft werden, ob die Mitarbeiter mit dem Sollkonzept konform agieren.
- Beim **Prinzip der Mindestinformation** („*need to know*“) geht es darum, dass Mitarbeiter nicht mehr Informationen erhalten sollen als genau jene, die sie für ihre Arbeit benötigen.

Diese Prinzipien spiegeln sich nicht nur in den Prozessen wider, sondern auch in der Basis-IT-Infrastruktur und bei Applikationen wie ERP. Das Pendant zu IKS auf Geschäftsebene heißt im IT-Bereich *COBIT (Control Objectives for Information and Related Technology)*.

Handlungsfelder aus dem Kernbereich Bilanztheorie, Prüfungswesen und Organisation sind beispielsweise die **Archivierung** und die **Bereitstellung erforderlicher Informationen für die Finanzberichterstattung**.

Die **Archivierung** beschreibt die unveränderbare, vollständige, sichere, nachvollziehbare und langfristige Aufbewahrung und Wiederherstellung von Informationen. Dies geschieht anhand von Methoden, Techniken und Tools des *Enterprise Content Managements (ECM)*, das organisatorische Prozesse zur Verwaltung unterschiedlich strukturierter Informationen unterstützt. Die in diesem Kontext eingesetzten Prozesse und Systeme müssen regulatorische Transparenzanforderungen erfüllen, die sich häufig aus dem Handels- und dem Steuerrecht

ergeben. Hierzu zählt etwa die Einhaltung der Revisionssicherheit durch elektronische Archivsysteme. Aus geschäftlicher Sicht ermöglicht die Archivierung eine nachvollziehbare Aufbewahrung wichtiger Informationen und den Schutz der Reputation des Unternehmens.

Aufbauend auf der Archivierung relevanter Dokumente kann in Unternehmen die regelmäßige Bereitstellung von Rechnungslegungsunterlagen im Rahmen der **Finanzberichterstattung** erfolgen. Ein hohes Maß an Effizienz wird auch hier durch die Nutzung entsprechender Prozesse und Systeme erzielt. Anforderungen an die Finanzberichterstattung müssen durch diese Prozesse und Systeme umgesetzt und deren Einhaltung fortlaufend überprüft werden. Generell gelten wie schon bei der Archivierung hohe Anforderungen an die Transparenz des Transfers und der Haltung relevanter Daten.

6.2.5 Informations- und Transparenzpflicht

Die Erfüllung der Informations- und Transparenzpflicht umfasst verschiedene Aspekte. Aus interner Sicht stellt diese Pflicht hohe Anforderungen an die Prozesse und die bereichsübergreifende Zusammenarbeit im Unternehmen. Je nach Branchen können besondere Berichts- und Offenbarungspflichten gelten, welche Unternehmen bei der Gestaltung ihrer Infrastruktur und Prozesse berücksichtigen müssen. Auch Kunden- und Lieferantenverhältnisse ziehen spezielle Anforderungen nach sich.

Ein wichtiges Handlungsfeld der Informations- und Transparenzpflicht ist das **Vertragsmanagement**. Um Anforderungen, die aus Kunden- und Lieferantenvereinbarungen entstehen, nachvollziehbar und effizient zu verwalten und letztlich umzusetzen, müssen klare Richtlinien und gegebenenfalls einheitliche Vorlagen zur Vertragsgestaltung vorliegen. Im Hinblick auf *Outsourcing*-Vorhaben etwa hat eine einheitliche Gestaltung von *Sourcing*-Verträgen den Vorteil, dass allgemein geforderte Leistungsmerkmale an ausgelagerte Dienste einheitlich und transparent gehalten werden (zum Beispiel die Verfügbarkeitsquote von *Cloud*-Diensten).

Ein weiteres Handlungsfeld besteht in den Berichtspflichten, welchen Unternehmen je nach Branche oder für bestimmte Märkte unterliegen. Als allgemeines Beispiel kann hierfür die **Finanzberichterstattung** genannt werden, die im Rahmen des Bilanz- und Prüfungswesens eine wichtige Rolle spielt. Für die regulierten Bereiche sollten klare Zuständigkeiten existieren, mit denen die Erfüllung der Berichtspflichten abgedeckt wird. Auch hier gilt der Grundsatz, dass die Umsetzung und Überprüfung der Berichtsanforderungen anhand dokumentierter Prozesse und Systeme erforderlich und wichtig sind, um Transparenz gegenüber externen Anspruchsgruppen und Nachvollziehbarkeit der internen Abläufe zu gewährleisten.

6.2.6 Globalisierung und Transformation

Um das Innovationspotenzial der digitalen Transformation und der Erschließung globaler Märkte abzurufen, müssen Unternehmen ein hohes Maß an Flexibilität im Umgang mit Technologien und im Hinblick auf die eigene Organisationsstruktur an den Tag legen. Um Infrastruktur und Organisationsstruktur schnell an neue Technologien und notwendige Veränderungen anzupassen, müssen Verfahren etabliert sein, welche für die fortlaufende Einhaltung regulatorischer Anforderungen sorgen. Wichtige Handlungsfelder stellen dabei das **Technologiemanagement** und das **Management der Organisationsstruktur** dar.

Das **Technologiemanagement** beinhaltet die Analyse und Bewertung bestehender und neu aufkommender Technologien, unter anderem hinsichtlich ihres Nutzens, des Aufwands der Umsetzung sowie bei der Umsetzung zu beachtender regulatorischer Anforderungen (Stand der Technik). So muss beispielsweise vor dem Einsatz von *Cloud Computing* oder von *Big-Data*-Analyseverfahren geklärt werden, welche Auswirkungen der Einsatz auf die Einhaltung bestehender Regularien hat und ob sich aus dem Einsatz neue Verpflichtungen ergeben. Im Gegensatz zu konventionellen IT-Abteilungen, die sich mit Infrastrukturfragen beschäftigen, steht hier das Informationsmanagement im Zentrum.

Das **Management der Organisationsstruktur** beschäftigt sich in vergleichbarer Weise mit der Analyse und Bewertung anvisierter organisatorischer Veränderungen im Hinblick auf Nutzen, Aufwand und *Compliance*.

Beide Handlungsfelder sollten nicht ad hoc, sondern auf Basis klarer und unternehmensweiter Prozesse und Verfahren umgesetzt werden, um die Einhaltung regulatorischer Anforderungen fortlaufend sicherzustellen und um die infolge der hohen Dynamik der digitalen Transformation notwendige Handlungsschnelligkeit und Flexibilität zu erreichen. Damit werden Unternehmen befähigt, Transformations- und Globalisierungsvorhaben im globalen Wettbewerb schnell, effizient und unter Beachtung aller relevanten Regularien durchzuführen.



Analystenfazit:

Die Handlungsfelder des *Compliance*-Modells geben die „Stellschrauben“ vor, mit denen Prozesse verbessert und der Nutzen von *Compliance* in Bezug auf das eigene Unternehmen realisiert wird.

6.3 *Compliance*-Prozesse beurteilen und verbessern

Mit dem oben dargestellten Modell lassen sich zwei unterschiedliche Ansätze verfolgen. Beide dienen dazu, den Status der *Compliance* in der eigenen Organisation zu erfassen, zu bewerten und letztlich zu verbessern.

Der erste Ansatz verfolgt das in der ersten Ausgabe dieses Handbuchs vorgestellte Reifegradmodell. Bei diesem werden die „Reife“ und damit die Umsetzungsqualität der mit *Compliance* befassten Prozesse bestimmt. Je höher der Reifegrad, desto besser sind die sechs Ziele des Modells umgesetzt.

Der zweite Ansatz beruht auf einem von KPMG entwickelten *Self-Assessment*. Dieses umfasst die interaktive Beantwortung von Fragen zu den einzelnen Handlungsfeldern des Modells. Anhand der Antworten werden dann diejenigen Handlungsfelder bestimmt, die konkreten Verbesserungsbedarf aufweisen.

6.3.1 Ansatz 1: Nutzung eines qualitativen Reifegradmodells

In der Vorgängerversion dieses Handbuchs aus dem Jahr 2009 wurde ein **Reifegradmodell** eingeführt, das den Beitrag der IT-Infrastruktur zur Umsetzung von *Compliance* in vier Reifegradstufen misst.

Dieses Modell hat bis heute kaum an Relevanz eingebüßt. Im Gegenteil: In Zeiten, in denen immer neue Bereiche und Prozesse auf IT-Diensten und Technologien basieren, spielt die IT zwangsläufig auch für die Erfüllung regulatorischer Anforderungen eine immer zentralere Rolle. Die Auslagerung von IT-Diensten und -Infrastrukturelementen in die *Cloud* sorgt aber gleichzeitig dafür, dass zahlreiche Aspekte des Reifegrades von IT-Infrastrukturen mittlerweile durch externe *Cloud*-Dienstleister erbracht werden können. Der Funktion der lokalen IT, Infrastrukturkomponenten zur Unterstützung operativer Anforderungen bereitzustellen, kommt deshalb eine geringere Bedeutung zu, als es vor acht Jahren der Fall war.

Aus diesem Grund soll an dieser Stelle darauf verzichtet werden, erneut die Reife der IT-Infrastruktur in einem **Reifegradmodell** abzubilden. Stattdessen soll der Frage nachgegangen werden, ob und wie Unternehmen ihre internen Strukturen und Prozesse bewerten und verbessern können, um die Ziele des *Compliance*-Modells zu erreichen.

In der Literatur gibt es verschiedene **Reifegradmodelle**, die manchmal auch als Prozessbefähigungsmodelle bezeichnet werden. Mit diesen Modellen lässt sich die Güte von Prozessen messen. Die Grundidee stammt ursprünglich aus dem Bereich der Softwareentwicklung. Mittels Reifegraden lässt sich überprüfen, wie gut der Prozess der Softwareentwicklung und damit letztlich auch die Software selbst ist. Das Modell lässt sich aber auch gut für die Messung der Qualität anderer Prozesse einsetzen – etwa für den Umgang mit *Compliance*-Anforderungen.

Im Folgenden soll das weit verbreitete **Reifegradmodell *Capability Maturity Model Integration (CMMI)*** eingesetzt werden. Die Abbildung und Tabelle zeigen die fünf Stufen des Modells:

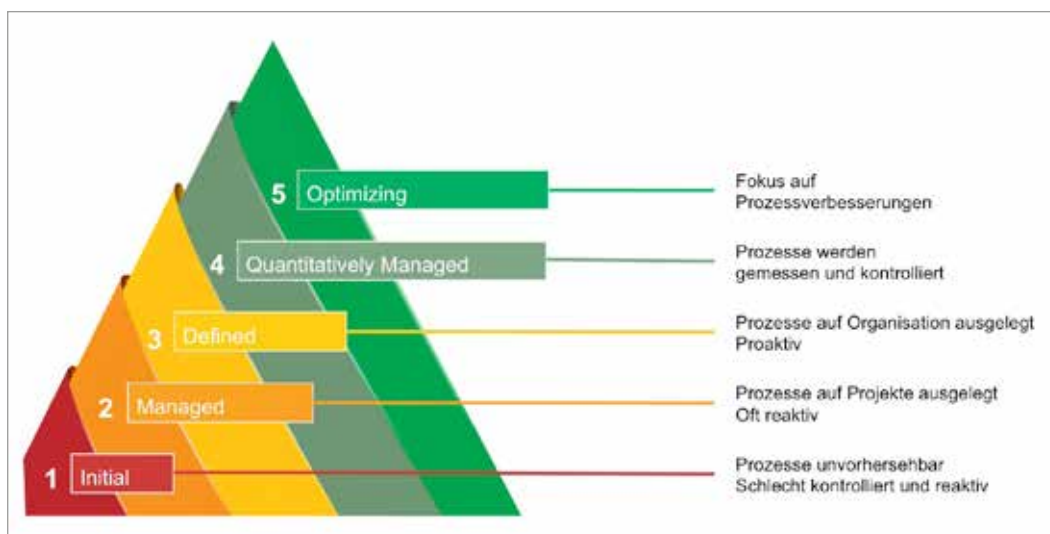


Abbildung 16: CMMI-Reifegradmodell

Stufe	Bedeutung
1	Die niedrigste Reifegradstufe, die es zu erreichen gilt, ist die 1 (initial). Die Prozesse werden ad hoc abgewickelt. Projekterfolge beruhen in erster Linie auf den Fähigkeiten des Projektleiters. Bei einem anderen Projektleiter könnte dasselbe Projekt ein Misserfolg werden. Planungen sind unvollständig, eine konsequente Erfolgskontrolle gibt es nicht.
2	Stufe 2 bringt gegenüber Stufe 1 einige Fortschritte in Bezug auf das Projektmanagement. Stufe 2 wird erreicht, wenn die grundlegenden Projektmanagementprozesse zur Planung und Steuerung von Zeit und Kosten etabliert sind. Dabei reicht es aus, wenn diese Prozesse rudimentär implementiert sind. Wichtig ist, dass die Prozesse auch tatsächlich „gelebt“ werden.
3	Ab Stufe 3 geht es nicht mehr um einzelne Prozesse, sondern um die Organisation als Ganzes. Innerhalb der Firma oder Behörde müssen die Prozesse einheitlich standardisiert werden. Darüber hinaus ist eine Dokumentation der Prozesse erforderlich.
4	Für Stufe 4 müssen die Prozesse innerhalb der Organisation vereinheitlicht werden. Zudem ist es erforderlich, dass die Qualität der Prozesse über <i>KPIs (Key Performance Indices)</i> gemessen und daraus Vorhersagen für den Projektverlauf getroffen werden.
5	In der höchsten Stufe 5 müssen die Prozesse kontinuierlich verbessert werden. Ein Hilfsmittel dazu ist die regelmäßige Suche nach Schwachstellen in den Prozessen.

Abbildung 17: Beschreibung der CMMI-Reifegradstufen

Es stellt sich die Frage, welchen Reifegrad Prozesse haben müssen, um im täglichen Geschäftsablauf akzeptabel zu sein. Das Endziel ist natürlich ein Reifegrad von 5 für alle Prozesse, doch diesen Zielwert wird man in der Praxis kaum erreichen.

Ein Beispiel für praxisgerechte Reifegrade ist die Zertifizierung eines Managementsystems – beispielsweise ein Informationsmanagementsystem nach ISO 27001. Für eine Erstzertifizierung müssen dessen Prozesse einen Reifegrad von 3 oder höher aufweisen. Bei jeder Re-Zertifizierung wird dann ein Reifegrad angestrebt, der höher liegt als beim letzten Audit. Dabei lässt sich über eine Automatisierung von *Workflows* mit vergleichsweise kleinem Aufwand ein höherer Reifegrad erreichen – einer der Vorteile der digitalen Transformation.

Ein angenehmer Nebeneffekt bei der Erhöhung von Reifegraden ist die Verringerung von Kosten für einen Prozess. Allerdings ist die Beziehung zwischen Reifegrad und Prozesskosten nicht linear. Im Gegenteil: Soll der Reifegrad erhöht werden, muss zunächst Geld in die Hand genommen werden, etwa für entsprechende Projekte oder für den Kauf einer Software. Im Endeffekt wird jedoch Geld gespart, wie die folgende Abbildung verdeutlicht.

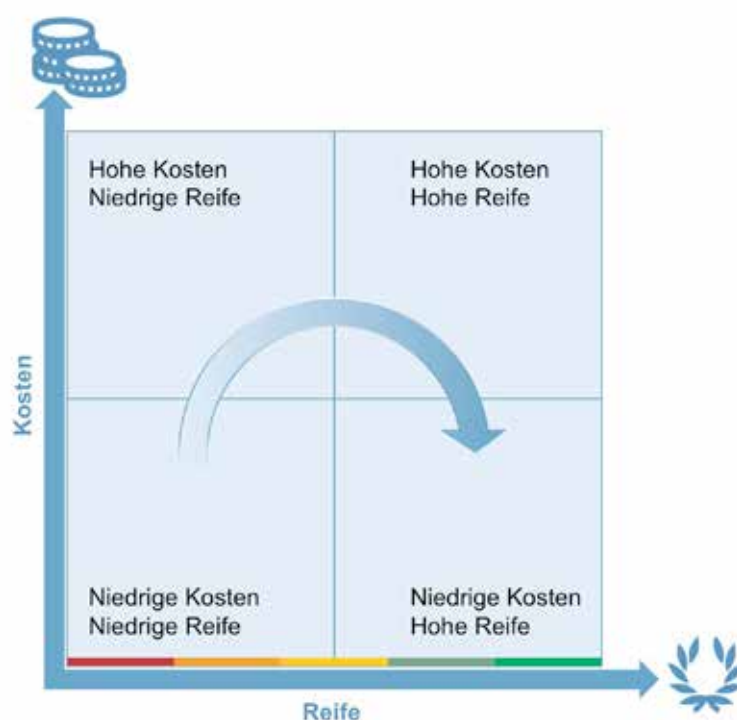


Abbildung 18: Prozessreife und Prozesskosten

Auch die Definition von *Compliance*-Anforderungen und deren Umsetzung umfasst Geschäftsprozesse, deren Qualität sich mit einem **Reifegradmodell** messen lassen. Entscheidungsträger stellen sich dabei einerseits die Frage nach dem Status quo – also dem aktuellen Reifegrad der *Compliance*-Prozesse in ihrem Unternehmen – und nach möglichen Handlungsfeldern, also konkreten Verbesserungsmöglichkeiten und daraus resultierenden Aufgaben, die das Erreichen eines höheren Reifegrades ermöglichen sollen.

Das beschriebene **Reifegradmodell** kann wie folgt zum Einsatz kommen:

1. Im ersten Schritt werden die für die eigene Organisation wichtigen Handlungsfelder ermittelt. Dabei können die im Modell angegebenen Beispielhandlungsfelder als Vorgaben und Inspirationsquellen genutzt werden. Es ist darauf zu achten, dass jeder der sechs Kernbereiche durch mindestens zwei Handlungsfelder repräsentiert wird bzw. dass sich existierende Organisationseinheiten im Handlungsfeldmodell wiederfinden.
2. Anschließend sind die Prozesse zu ermitteln, durch die diese Handlungsfelder bearbeitet werden. Dabei sollte jeder Prozess mit seinen Schnittstellen zu anderen Prozessen beschrieben werden. Außerdem muss neben Zuständigkeiten und Rollen ebenso dokumentiert werden, welche Informationen im Prozess verarbeitet werden und wie der Datenfluss über die Schnittstellen ist.
3. Dann wird jeder Prozess dahingehend bewertet, wie sein Reifegrad ist. Diese Bewertung findet qualitativ nach den Kriterien des **CMMI-Reifegradmodells** statt. Die Reifegradstufen jedes Prozesses werden mit der Begründung für die Einstufung in die Dokumentation aufgenommen.
4. Der Reifegrad jedes Kernbereichs wird durch das arithmetische Mittel der Reifegrade aller Prozesse ermittelt, die die Handlungsfelder des jeweiligen Kernbereichs bearbeiten.
5. Kernbereiche mit einem Reifegrad von 3 oder weniger sind dahingehend zu untersuchen, wie die den Handlungsfeldern zugeordneten Prozesse verbessert werden können.
6. Befinden sich innerhalb eines Kernbereichs Prozesse mit stark unterschiedlichem Reifegrad, so besteht ebenfalls Handlungsbedarf. Im Idealfall haben alle mit *Compliance* befassten Prozesse einen sehr ähnlichen Reifegrad. Zurückgebliebene Prozesse sind mit Priorität zu verbessern und in ihrem Reifegrad zu steigern.

Analystenfazit:

Mit dem *Compliance*-Modell lässt sich eine qualitative Messung des Reifegrades von *Compliance*-Prozessen durchführen. Daraus lassen sich Verbesserungspotenziale ableiten, mit denen der Reifegrad weiter gesteigert wird.



6.3.2 Ansatz 2: *KPMG Self-Assessment*

Anhand einer Reifegradbewertung können sich Organisationen ein Bild vom Reifegrad ihrer *Compliance*-Prozesse machen und gegebenenfalls Verbesserungsprozesse identifizieren. Um eine tatsächliche Verbesserung zu erreichen, müssen dann allerdings konkrete Maßnahmen ergriffen werden. Dabei muss ein ganzheitliches Bewertungsschema vorliegen, das alle relevanten *Compliance*-Anforderungen beinhaltet. Existenz und Reifegrad der Prozesse, welche die jeweiligen Anforderungen umsetzen, werden dabei systematisch abgefragt. So entsteht ein Gesamtbild der *Compliance* unter Betrachtung aller relevanten Prozesse. Weiterhin muss eine Ergebnisanalyse stattfinden, aus der sich Handlungsfelder und letztlich konkrete Maßnahmen zur Verbesserung bestimmter *Compliance*-Prozesse herleiten lassen.

Einen solchen Ansatz verfolgt das *KPMG Self-Assessment*. Es basiert auf einem Online-Fragebogen, über den der Reifegrad und die Ausprägtheit von Prozessen der einzelnen Kernbereiche und Handlungsfelder bestimmt werden. Hierzu verwendet KPMG das oben skizzierte *Compliance*-Modell. Die fachspezifische Bewertung der *Compliance*-Umsetzung im Unternehmen erfolgt mit Hilfe von zahlreichen Detailfragen zu jedem Handlungsfeld. Das *Assessment* ist so ausgelegt, dass Verantwortliche aus unterschiedlichen Fachbereichen Fragen zu den Handlungsfeldern beantworten, die in ihren Bereich fallen. Das *Assessment* kann einfach und rollenbasiert über ein Onlineportal durchgeführt werden.

Die in den Fragen behandelten Aspekte aller Kernbereiche werden entweder anhand von Ja/Nein-Antworten oder auf einer mehrstufigen Skala von 1 bis 5 abgefragt. So lassen sich konkrete Bewertungen zu Fragen und Kernbereichen messen und aggregieren, die ähnlich wie beim Einsatz eines **Reifegradmodells** generalisierte Aussagen über den Reifegrad der Umsetzung eines Kernbereichs oder eines Teilaspekts zulassen. Die folgende Abbildung zeigt beispielhafte Fragen des **Assessments**, die zum Kernbereich Informations- und Kommunikationsmanagement gehören und thematisch in drei weitere Untergruppen untergliedert sind.

Die Ergebnisse des *Assessments* werden unter Anwendung eines Punktemodells bestimmt. Die Punkte gehen auf das Konto des Kernbereichs, welchem die jeweilige Frage zugeordnet ist. Die Ergebnisvisualisierung erfolgt anhand eines Spinnendiagramms, dessen Achsen durch die Kernbereiche bestimmt sind. Wie in der folgenden Abbildung eines Beispieldiagramms veranschaulicht wird, verschafft diese Darstellung einen schnellen Überblick über die Analyseergebnisse, mit denen eine Dringlichkeitseinschätzung basierend auf Prioritäten und einem Benchmark zum Vergleich mit anderen Organisationen möglich ist.

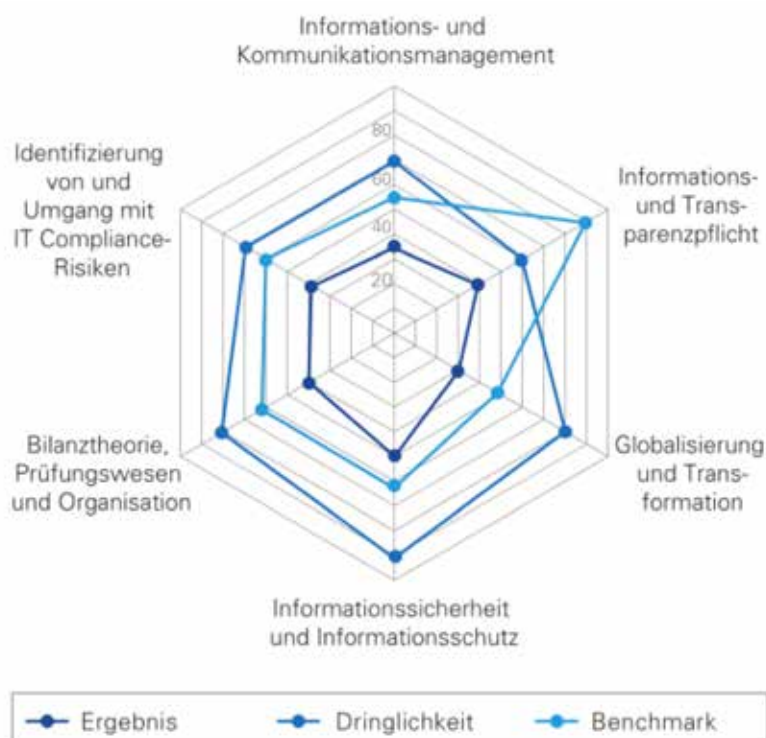


Abbildung 19: KPMG Self-Assessment – Grafische Darstellung der Analyseergebnisse (Beispiel)

Auf Basis der Analyseergebnisse werden Handlungsfelder bestimmt, aus denen Unternehmen und Organisationen konkrete Verbesserungsmaßnahmen für ihre Prozesslandschaft und Infrastruktur herleiten können. Hierzu bietet KPMG neben der fragen- und punktebasierten Bewertung und Analyse durch das *Self-Assessment* auch ein vertiefendes *Enhanced Assessment* zur expertengestützten Analyse der Ergebnisse unter Berücksichtigung branchenspezifischer Anforderungen an. Die Vertiefung besteht etwa in der Priorisierung der identifizierten Handlungsfelder basierend auf gesetzlichen Regularien, der Unterstützung bei der branchenspezifischen Ergebnisanalyse sowie der Erarbeitung konkreter Handlungsempfehlungen und Lösungsvorschläge. Im Abschlussgespräch werden praxiserprobte Lösungsvorschläge vorgestellt.

Analystenfazit:

Wird das *Compliance-Modell* zusammen mit dem *KPMG Self-Assessment* eingesetzt, ist eine quantitative und qualitative Bewertung der eigenen *Compliance-Prozesse* möglich. Weitergehende Vertiefungen führen zu konkreten Handlungsempfehlungen und Lösungsvorschlägen.



KAPITEL 7

67

BEITRAG DER *CLOUD* ZU *COMPLIANCE* UND GESCHÄFTSERFOLG

7. BEITRAG DER *CLOUD* ZU *COMPLIANCE* UND GESCHÄFTSERFOLG

In diesem Kapitel wird anhand eines technischen Modells strukturiert dargestellt, welche Zuständigkeiten im Rahmen der *Cloud*-Nutzung vom *Cloud*-Kunden an den *Cloud*-Anbieter übertragen werden und welche Vorteile sich hieraus aus *Compliance*-Sicht für den Kunden ergeben können. In Abschnitt 7.1 werden hierzu die *Cloud-Service*-Modelle und das klassische *Hosting* zunächst gegenübergestellt und voneinander abgegrenzt. Darüber hinaus wird die wichtige Kontrollfunktion von *Service Level Agreements* erläutert. In Abschnitt 7.2 werden *Compliance*-Vorteile beispielhaft in Anlehnung an zwei Kernbereiche des *Compliance*-Modells dargestellt. Die Ergebnisse werden in Abschnitt 7.3 allgemein diskutiert.

Mit der Verlagerung von Geschäftsprozessen in die digitale Welt nimmt die Bedeutung der Informationstechnik zwar zu, die der klassischen Betreiber-IT jedoch ab. Die technischen Lösungen werden durch *Cloud*-Anbieter bereitgestellt, die interne IT wird sich eher mit der digitalen Gestaltung von Geschäftsprozessen beschäftigen und damit, ein Informationsmanagement abzubilden und zu unterstützen sowie *Cloud*-Dienste zu überwachen. Das gilt auch insbesondere für die mit *Compliance* zusammenhängenden Prozesse, bei denen cloudbasierte Ansätze Teil des internen Kontrollsystems werden.

7.1 *Cloud-Service*-Modelle im Vergleich

Bereits in Kapitel 4 wurden mögliche Nutzenpotenziale der *Cloud*-Nutzung aus Sicht der *Compliance* erläutert. Dabei wurde insbesondere der Transfer der Zuständigkeit für die Auditierung und Zertifizierung technischer und organisatorischer Sicherheitsmaßnahmen vom Kunden zum Anbieter und die damit einhergehende höhere Flexibilität von Unternehmen bei der (Um-)Gestaltung ihrer Prozesse und Systeme hervorgehoben. Im folgenden Abschnitt werden zunächst gängige *Cloud*-Dienstmodelle erläutert und mit klassischen Modellen der IT-Bereitstellung verglichen. Im Anschluss wird dargestellt, inwiefern Zuständigkeiten für die technische und organisatorische Umsetzung von *Compliance* zum Anbieter transferiert werden können und welche Vorteile sich daraus aus *Compliance*-Sicht ergeben.

7.1.1 Übertragung von Zuständigkeiten

Bei der eigenständigen *Inhouse*-Bereitstellung einer Anwendung liegen die Zuständigkeiten für Implementierung, Umsetzung und Instandhaltung von Kontrollen beim Unternehmen selbst. Bei einer cloudbasierten Bereitstellung teilen sich *Cloud*-Anbieter und Kunde diese Zuständigkeiten. Maßgeblich für den Grad der Abgabe derartiger Zuständigkeiten an den Anbieter ist das angewendete *Cloud*-Dienstmodell.

IT-Leistungen werden immer mehr durch externe Dienstleister erbracht. Dazu zählen bereits klassische *Hosting*-Dienste, welche die Bereitstellung von Servern für ihre Kunden übernehmen. Eine wichtigere Rolle spielen jedoch *Cloud*-Dienste, die ihren Kunden je nach *Cloud*-Modell Infrastrukturdienste, Platfordmdienste oder gleich gesamte Softwareapplikationen bereitstellen. Die Wahl des *Cloud*-Modells stellt dabei für Unternehmen keine rein technische, sondern eine strategische Entscheidung dar, die entscheidende Auswirkungen auf Infrastruktur, Prozesse und nicht zuletzt auch auf die Umsetzung von *Compliance* hat. In der folgenden Darstellung werden die drei verbreitetsten *Cloud*-Modelle erläutert und der internen *Inhouse*-Bereitstellung sowie dem klassischen *Hosting* hinsichtlich der Verteilung technischer Zuständigkeiten zwischen Dienstanbieter und -kunde gegenübergestellt.

Eigene IT	Hosting	IaaS	PaaS	SaaS
Daten	Daten	Daten	Daten	Daten
Anwendungen	Anwendungen	Anwendungen	Anwendungen	Anwendungen
Datenbanken	Datenbanken	Datenbanken	Datenbanken	Datenbanken
Betriebssysteme	Betriebssysteme	Betriebssysteme	Betriebssysteme	Betriebssysteme
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Serverinfrastruktur	Serverinfrastruktur	Serverinfrastruktur	Serverinfrastruktur	Serverinfrastruktur
Netzwerk- und Datenspeicher	Netzwerk- und Datenspeicher	Netzwerk- und Datenspeicher	Netzwerk- und Datenspeicher	Netzwerk- und Datenspeicher
Datencenter	Datencenter	Datencenter	Datencenter	Datencenter
Erbringung durch Dienstkunden Erbringung durch Dienstanbieter				

Abbildung 20: Aufteilung der Zuständigkeiten zwischen *Cloud*-Anbieter und -Kunde

Vom klassischen *Server Hosting* unterscheidet sich die *Cloud* in erster Linie durch den Einsatz von Virtualisierungstechnologien. Im Gegensatz zu *Hosting*-Anbietern stellen *Cloud*-Anbieter also keine dedizierten Server mehr bereit, die physisch vom Kunden genutzt und konfiguriert werden. Kunden erhalten vielmehr Zugriff auf virtuelle Instanzen, die über ein oder mehrere Datencenter verteilt betrieben und zentral angesteuert werden können. Während Systeme und Daten beim *Hosting* also auf einem physisch vorhandenen Server verweilen und an dessen Kapazitäten gebunden sind, können Ressourcen wie Speicher, Hardware oder auch verfügbare Instanzen in der *Cloud* nahezu beliebig skaliert werden.

Der Einsatz von Virtualisierung stellt eine der wesentlichen technischen Innovationen der *Cloud* gegenüber klassischen *Outsourcing*-Vorhaben wie *Hosting* oder *Collocation* dar. Durch den Einsatz von Virtualisierung werden nicht nur verbesserte Infrastrukturdienste im *IaaS*-Modell, sondern auch deutlich komplexere Plattform- und Softwaredienste im *PaaS*- bzw. *SaaS*-Modell ermöglicht.

- Im **IaaS-Modell** erfolgt die Bereitstellung einer sicheren und überprüfbaren Server-, Netzwerk und Hostinfrastruktur innerhalb des Datencenters durch den *Cloud*-Anbieter. Diese Infrastruktur ermöglicht die Bereitstellung von Rechenkapazitäten, Netzwerkanbindung und der nötigen Hard- und Softwarekomponenten zur Datenablage und zur Implementierung virtueller Maschinen.
- Im **PaaS-Modell** stellt der *Cloud*-Anbieter nicht nur die Hardware-Infrastruktur bereit, sondern darüber hinaus grundlegende Software in Form von Entwicklungs-umgebungen und Schnittstellen. Auf deren Basis können Kunden eigene Systeme installieren, Software entwickeln und bereitstellen.
- Im **SaaS-Modell** wird eine Software vom Anbieter auf seiner *Cloud*-Infrastruktur betrieben und vom Kunden als Dienstleistung – in der Regel über das Internet – bezogen. Für die Nutzung der Software reicht in vielen Fällen ein Internetbrowser aus.

Die unterschiedlichen Leistungsmerkmale der drei *Cloud*-Modelle gehen einher mit einer unterschiedlichen Aufteilung der Zuständigkeiten für die Gestaltung der Dienste unter Einhaltung regulatorischer und geschäftlicher Anforderungen. Auch wenn nach wie vor der *Cloud*-Kunde die Verantwortung für die Nutzung der Dienstleistung mit allen Konsequenzen trägt, birgt der Transfer technischer und organisatorischer Zuständigkeiten gerade aus *Compliance*-Sicht viele Vorteile.



Analystenfazit:

Ein *Cloud*-Kunde kann einen Teil seiner Zuständigkeiten im Sinne von *Compliance*-Anforderungen an den *Cloud*-Anbieter übertragen. Es hängt vom gewählten *Cloud*-Modell ab, wie umfangreich diese Übertragung sein kann.

7.1.2 Steuerung des Anbieter-Kunden-Verhältnisses

Bei der Betrachtung der Vereinbarungen über die *Cloud*-Nutzung, die Kunde und Anbieter in aller Regel treffen, werden bereits erste Nutzenpotenziale deutlich. In *Service Level Agreements* (SLAs) und Dienstleistungsbedingungen („*Service Terms*“) werden Leistungsmerkmale und -kontrollen fixiert. Über diese Vereinbarungen kann der *Cloud*-Kunde steuern, in welcher Qualität und Intensität ein *Cloud*-Anbieter Dienste erbringt.

Bestandteile dieser Vereinbarungen sind etwa:

- Verfügbarkeitsgarantien seitens des Anbieters
- Vorgaben für den Datenschutz
- Vorgaben für den Ort der Datenhaltung und -verarbeitung
- Vorgaben zur Überprüfbarkeit und Auditierung von Diensten und Infrastruktur
- Vorgaben für die korrekte Nutzung von Diensten
- Verantwortlichkeiten bei der Nutzung von Diensten sowie
- Haftungsübernahmen und -begrenzungen

Die Aufteilung der Verantwortlichkeiten wird erleichtert, wenn die beteiligten Partner ihre unternehmensinternen Prozesse an gängigen Standards ausrichten. Das können beispielsweise COSO, COBIT oder die Informationssicherheitsstandards ISO 27001 oder 27002 sein. Damit spricht man eine gemeinsame Sprache und hat ein gemeinsames Verständnis. Übergangspunkte von Prozessen und die dazu benötigten Protokolle lassen sich dann leichter definieren, umsetzen und kontrollieren.

7.2 Anwendungsbeispiele

Betrachtet man die Eigenschaften und Leistungsmerkmale der *Cloud* unter Berücksichtigung der drei unterschiedlichen *Cloud*-Modelle, so wird deutlich, dass gerade die Nutzung von Plattform- und Softwarediensten (*PaaS* bzw. *SaaS*) zur Einhaltung regulatorischer Anforderungen und zur Erreichung eines hohen Maßes an Flexibilität im Hinblick auf zukünftige Veränderungen beiträgt. Warum dem so ist, soll im Folgenden beispielhaft anhand zweier Kernbereiche beschrieben werden.

7.2.1 *Compliance*, Informationssicherheit und -schutz

Die Sicherheit von Daten, Systemen und Informationen muss organisatorisch und technisch für Hardware, Software und die zugrunde liegende Infrastruktur sichergestellt werden. Dazu existieren regulatorische Anforderungen und Standards, deren Einhaltung überwacht werden muss. Betrachtet man zunächst die einfache *On-Premises*-Bereitstellung, so wird schnell klar, dass alle Sicherheits- und Schutzmaßnahmen vom Unternehmen selbst getroffen, koordiniert, umgesetzt, überwacht und fortlaufend gemäß der Bedrohungslage und dem Stand der Technik aktualisiert werden müssen. Besonders für kleinere und mittelständische Unternehmen stellt dies eine große finanzielle und organisatorische Herausforderung dar. Wie würde sich die Nutzung eines der drei *Cloud*-Modelle für das Unternehmen bezahlt machen?

Das *IaaS*-Modell

Mit dem *IaaS*-Modell delegiert ein Unternehmen die Aufgabe der Bereitstellung einer sicheren, zertifizierten und sich auf dem Stand der Technik befindlichen Datencenter-, Server-, Netzwerk- und Hostinfrastruktur an einen *Cloud*-Anbieter. Die Einhaltung von Normen, Regularien und Standards zum Betrieb des Rechenzentrums, der Server und der Netzwerkanbindung wird also vom *Cloud*-Anbieter übernommen. Notwendige Aktualisierungen werden vom *Cloud*-Anbieter durchgeführt, ohne dass auf Kundenseite beispielsweise neue Hardware angeschafft oder neues Sicherheitspersonal eingestellt oder geschult werden muss. Auch bei Datenwiederherstellung und Notfallmanagement profitiert der *Cloud*-Kunde von der Infrastruktur des Anbieters. Viele *Cloud*-Anbieter bieten hier mehrere Optionen an, etwa die lokale redundante oder die georedundante Speicherung von Daten in Datencentern in verschiedenen Regionen. Da der im Wettbewerb mit Konkurrenten stehende *Cloud*-Anbieter selbst ein großes Interesse daran hat, sich nach etablierten Sicherheitsstandards zertifizieren zu lassen, profitiert der *Cloud*-Kunde zudem von der fortlaufend überprüften Einhaltung gängiger und hoher Sicherheitsstandards durch den *Cloud*-Anbieter.

Das *PaaS*-Modell

Beim *PaaS*-Modell werden neben der Infrastruktur auch die Sicherheit der für den Betrieb einer Plattform notwendigen Software – etwa Betriebssysteme und Datenbanksysteme – durch den *Cloud*-Anbieter bereitgestellt. Hierdurch werden Umsetzung und Überprüfung softwareseitiger Sicherheitsmaßnahmen an den *Cloud*-Anbieter delegiert. Dies gilt etwa für die Umsetzung eines Identitäts- und Zugriffsmanagements, die Bereitstellung sicherer Verschlüsselungsprotokolle und die Forcierung der Einhaltung guter Entwicklungspraktiken. Das *PaaS*-Modell ermöglicht einem Kunden also den Aufbau eigener Applikationen auf einer fortlaufend überprüften und vertrauenswürdigen Infrastruktur- und Softwareplattform. Dadurch erhalten Entwickler auf Kundenseite eine standardisierte und fortlaufend überwachte Basis für die Implementierung eigener Applikationen.

Oft können *PaaS*-Kunden dabei bereits auf Sicherheitszertifizierungen des Anbieters aufbauen. Auf Plattformebene stellen viele *Cloud*-Anbieter zudem spezielle Tools und Dienste bereit, die dem Kunden die Möglichkeit geben, ein höheres Maß an Sicherheit zu erzielen. Dazu zählen beispielsweise Tools zur Schwachstellenanalyse oder zur Analyse und Klassifizierung von Daten nach ihrem Schutzbedarf.

Das *SaaS*-Modell

Die Nutzung des *SaaS*-Modells bedeutet den weitreichendsten Transfer von Zuständigkeiten vom *Cloud*-Kunden zum Anbieter. Da die gesamte Anwendung vom Anbieter bereitgestellt wird, entfällt auf Kundenseite sogar die Entwicklung der Applikation. Damit gehen weiterführende Sicherheits- und *Compliance*-Kontrollen bezüglich der Software in den Aufgabenbereich des Anbieters über. Unter anderem zählen hierzu etwa die kostspielige Überprüfung der Software auf Sicherheitslücken sowie die Bereitstellung fortlaufender Aktualisierungen und Updates. Nutzer von *SaaS*-Anwendungen erreichen ein sehr hohes Maß an Flexibilität, da das Portfolio an IT-Diensten, welche über *SaaS* bezogen wird, sehr einfach skaliert oder ergänzt werden kann, ohne dass dabei weitere Investitionen in Infrastruktur, Entwicklung oder Zertifizierungen anfallen. Audits und Zertifizierungen, die sich direkt auf die Sicherheit der Hardware- und Softwarekomponenten beziehen, werden vom *Cloud*-Anbieter erbracht.



Analystenfazit:

Ein *Cloud*-Kunde kann seine Informationssicherheit auf der seines *Cloud*-Anbieters aufbauen. Damit spart der Kunde eigene Ressourcen und erreicht trotzdem ein hohes Maß an Sicherheit.

7.2.2 *Cloud*-Dienste für mehr Dynamik und Flexibilität

Der Kernbereich Globalisierung und Transformation zielt auf eine hohe Flexibilität der Organisation sowie der technischen Infrastruktur ab, um schnelle Anpassungen an technische Innovationen vorzunehmen. Dies bedeutet auch, dass die vorhandene Infrastruktur anpassbar und skalierbar sein muss und sich die Änderungskosten in Grenzen halten. Hierin liegt eine der Schlüsselkompetenzen der *Cloud*, da Hardwareleistung und Softwarekomponenten von der zugrunde liegenden Infrastruktur abstrahiert und als Dienst bereitgestellt werden.

Der Beitrag der *Cloud* beschränkt sich nicht nur auf die Bereitstellung skalierbarer Hardwareressourcen. Denkt man den Grundgedanken von *Cloud Computing* konsequent zu Ende, so gelangt man zu der Erkenntnis, dass gerade in der Bereitstellung standardisierter Entwicklungsumgebungen oder ganzer Software-Pakete „*as a Service*“ eine große Chance für Unternehmen liegt. Diese können die technologische Basis ihres Erfolges wandelbar und ohne zusätzlichen Kostenaufwand gestalten. Die Nutzung der drei *Cloud*-Modelle macht sich dabei schon unter Gesichtspunkten der Transformierbarkeit aufgrund von Innovationen und Globalisierungsbestrebungen bezahlt.

Das *IaaS*-Modell

Die eigenständige *On-Premises*-Bereitstellung einer IT-Infrastruktur bremst die Anpassbarkeit der Organisation hinsichtlich neuer Technologien in vielerlei Hinsicht aus. Ändern sich die Anforderungen an die IT-Infrastruktur, mündet dies oft in teuren und zeitaufwendigen Investitionen. Technologische Anpassungen oder regulatorische Vorschriften können auch dazu führen, dass angeschaffte Hardware obsolet wird, Kapazitäten nicht ausreichen oder Standards nicht oder nur unzureichend erfüllt werden.

Bereits die Nutzung der *Cloud* im *IaaS*-Modell ermöglicht es, Hardwareressourcen als beliebig skalierbaren Dienst in Anspruch zu nehmen. Kosten und Zeitaufwand für die Bereitstellung und Wartung der Infrastruktur entfallen. Die infrastrukturelle Grundlage für IT-Innovationen wird also im wahrsten Sinne des Wortes „per Mausklick“ durch die Buchung von *IaaS*-Ressourcen geschaffen. Die Einhaltung von Regularien in Bezug auf die Hardware-Infrastruktur wird dabei, wie bereits beispielhaft für die Anforderungen des Informationsschutzes beschrieben, in den meisten Fällen vom *Cloud*-Anbieter umgesetzt.

Das *PaaS*-Modell

PaaS-Anbieter unterstützen Kunden durch eine einheitliche Plattform, die häufig eine Vielzahl an Softwarekomponenten wie Betriebssysteme oder Datenbanksysteme umfasst. Gleichzeitig werden oft Dienste bereitgestellt, die Kundenvorhaben unterstützen und einzeln gebucht werden können. Neben den Vorteilen durch die Bereitstellung der Infrastruktur ermöglicht das *PaaS*-Modell den Kunden eine effizientere Entwicklung und Implementierung eigener Lösungen auf Basis allgemeingültiger Standards. Regulatorische Anforderungen und Standards unterschiedlicher Branchen werden von *PaaS*-Anbietern häufig durch Dienste und in der Architektur der Plattform selbst umgesetzt, so etwa Überwachungs-, Diagnose- oder Analysetools. Dies beschleunigt die Entwicklung individueller Kundenlösungen und vereinfacht *Compliance* durch die Standardisierung der Softwarelandschaft. Insgesamt wird im *PaaS*-Modell sowohl im Hinblick auf die eingesetzte, eigenständig entwickelte Software als auch hinsichtlich der Anpassbarkeit der Softwarelandschaft an veränderte Anforderungen ein hohes Maß an Flexibilität erreicht.

Das *SaaS*-Modell

Da im *SaaS*-Modell komplette Softwarekomponenten als *Cloud*-Dienst bezogen werden, bietet dieses Modell das höchste Maß an Anpassbarkeit hinsichtlich veränderter Anforderungen. Ändern sich die Anforderungen an eine Softwarekomponente, so besteht keinerlei software- oder hardwaretechnischer Veränderungsbedarf mehr. Die *SaaS*-Nutzung kann einfach skaliert werden, etwa hinsichtlich Rechenleistung oder Benutzeranzahl. Ferner können einfach und bedarfsgerecht Dienste hinzugebucht oder abbestellt werden. Da die Software als Ganzes vom Anbieter bereitgestellt wird, obliegt auch deren Auditierung und Zertifizierung dem Anbieter. Während Änderungen an eigenständig bereitgestellter *On-Premises*-Software häufig neue Auditierungen und Zertifizierungen notwendig machen, entfällt dieser Aufwand im *SaaS*-Modell. Sofern ein *Cloud*-Anbieter über ein passendes Portfolio an *SaaS*-Diensten verfügt, können Unternehmen ihre Softwarelandschaft bequem um adäquate Standardlösungen für allgemeine oder branchenspezifische Fälle ergänzen. *Cloud*-Kunden können darauf verzichten, eigene aufwendige Investitionen zu tätigen, die unter funktionellen und regulatorischen Gesichtspunkten fortlaufend Veränderungen unterliegen.

Analystenfazit:

Cloud-Dienste sind flexibel und skalierbar. Deshalb ist ihr Nutzwert im Hinblick auf die Anforderungen der digitalen Transformation sehr hoch.



7.3 Die *Cloud* als Win-win-Strategie

Für ein Unternehmen, das sich zum Einsatz einer *Cloud*-Lösung entschließt, ergibt sich ein großer Nutzen. Man profitiert von den Vorteilen der digitalen Transformation, gleichzeitig werden *Compliance*-Anforderungen besser erfüllt, und als Folge davon wird der Reifegrad der eigenen Geschäftsprozesse erhöht. Zudem kann in einer *Cloud* ein höherer Grad an Informationssicherheit erreicht werden, als dies in einem normalen Rechenzentrum eines kleinen oder mittleren Unternehmens der Fall sein kann. Damit ergeben sich Vorteile auch für Prozesse, die nicht oder nur indirekt von der *Cloud* betroffen sind.

Der Nutzen liegt aber auch beim Anbieter von *Cloud*-Leistungen. Je mehr Kunden seine Dienste in Anspruch nehmen, desto besser können diese standardisiert werden. Dies führt zu Synergieeffekten, die sich aus dem Verkauf gleicher oder ähnlicher Leistungen an mehrere Kunden ergeben. Die gleiche Leistung kann dann effizienter angeboten werden.

Cloud-Anbieter profitieren aber auch beim Thema *Compliance* und Informationssicherheit. Schon aus Gründen der Konkurrenz muss jeder Anbieter für ein hohes Niveau an *Compliance* und Sicherheit sorgen und dies mittels Audits und Zertifizierungen nachweisen. Der Reifegrad der Geschäftsprozesse steigt beim Anbieter von Audit zu Audit ebenfalls an, mit denselben Vorteilen wie bei seinen Kunden.

Die obligatorischen Audits und Zertifizierungen haben dann wieder direkte Vorteile für die *Cloud*-Kunden. Den Nachweis, dass *Compliance*, Daten- und Informationsschutz im eigenen Unternehmen ausreichend umgesetzt werden, kann ein *Cloud*-Kunde mit Verweis auf die Zertifizierung seines Anbieters leicht erbringen. Nur in Ausnahmefällen muss der Kunde eigene Lieferanten-Audits bei seinem *Cloud*-Dienstleister in die Wege leiten.

Insgesamt entsteht durch die digitale Transformation und die *Cloud* als ihre Basistechnologie eine Win-win-Situation für alle Beteiligten. Das umfasst *Cloud*-Kunden und -Anbieter, aber auch Endkunden und Endnutzer, die von digitalisierten Prozessen profitieren und ihre privaten Ansprüche besser mit den Erfordernissen der Informationstechnik in Einklang bringen können.



Analystenfazit:

Cloud-Kunden und *Cloud*-Anbieter profitieren gleichermaßen von der *Cloud*. Der Reifegrad ihrer Geschäftsprozesse wird vergrößert, zudem können beide die Vorteile der digitalen Transformation für sich nutzen.

8. EPILOG

Ziel dieser Ausführungen ist es, aufzuzeigen, dass sich jedes Unternehmen – vom Start-up über den Mittelstand bis zum Global Player – und jede Behörde mit dem Thema *Compliance* konstruktiv und auch zum eigenen wirtschaftlichen Nutzen auseinandersetzen sollte und muss, denn faktisch ist es für jede Organisation eine Pflicht, gesetzliche und regulatorische Anforderungen zu erfüllen. Aber *Compliance* ist nicht nur eine Pflicht, sondern eine Verpflichtung.

Compliance gibt Maßnahmen vor, die garantieren, dass gesetzliche oder auch regulatorische Mindestanforderungen erfüllt werden, die auch in den Bereichen greifen, die gerne Sparmaßnahmen oder anderen Faktoren zum Opfer fallen oder einfach nicht berücksichtigt werden. Ein Grund hierfür ist beispielsweise der zusätzliche oder kostenintensive Aufwand, der sich unternehmensintern nur schwer rechtfertigen lässt. So steht beispielsweise im Niedrigpreissegment des *IoT* zu vermuten, dass aufgrund von Sparmaßnahmen einige wichtige Aspekte des Funktionsumfangs vernachlässigt würden, wenn nicht *Compliance*-Vorgaben dafür sorgen, dass ein bestimmtes Qualitätsniveau gehalten wird.

Setzen Organisationen ein **Compliance-Modell** um, können sie erreichen, dass Normen und Regeln einheitlich definiert und auch umgesetzt werden. Die Regulierungen bzw. Standardisierungen stellen sicher, dass der Ablauf wirtschaftlicher Prozesse transparent, kontrollier- und nachvollziehbar wird. Dies vereinfacht auch das Zusammenspiel der Unternehmen sowie den Aufbau von unternehmensübergreifenden Produktionsketten und erweiterten Serviceorganisationen. Die Basis einer Kooperation beruht damit nicht mehr nur auf Vertrauen und Selbstverständnis, sondern auch auf Klarheit und Wissen. Wird ein *Compliance*-Modell in einer Organisation zentral und einheitlich aufgebaut und umgesetzt, ist auch sichergestellt, dass alle *Workflows* regelkonform ineinandergreifen – und hierbei spielt *Cloud*-Technologie eine tragende Rolle.

Compliance-Informationen sind heute wichtige Metadaten zu Geschäftsdaten. Diese begleitenden Informationen geben den Geschäftsdaten einen zusätzlichen Wert, da sie eine automatisierte und rechtskonforme Weiterverarbeitung erst möglich machen. Mit dem gezielten und situationsgebundenen Austausch von *Compliance*-Informationen zwischen den Unternehmen können sie automatisierte Workflows abbilden, die der notwendigen Dynamik heutiger und künftiger Prozesse entsprechen. Ein Ausbau dieser Möglichkeiten – auch über die Grundlagen der *Compliance* hinaus – wird eine Voraussetzung für den Erfolg dieser vierten Wirtschaftsperiode sein.

Unternehmen und Behörden sollten jedoch nicht nur die *Compliance*-Anforderungen umfassend erfüllen, sondern ihre Investitionen auch nutzen, um ihre **Unternehmensziele** optimal erfüllen zu können. Dann greifen die Maßnahmen auch in nicht-regulierten Bereichen und schützen so den gesamten Wert von Forschung und Entwicklung, Produktion, Dienstleistung und Transaktionen und anderen wertschöpfenden Leistungen des Unternehmens.

Die **Bedeutung von Compliance** wird auch weiterhin zunehmen. Die Umsetzung und die Einhaltung von *Compliance*-Vorgaben sind wichtige strategische Aufgaben einer jeden Organisation. Ein entscheidender Erfolgsfaktor hierbei ist es, frühzeitig eine IT-Umgebung bereitzustellen, die anpassungsfähig und flexibel ist und die die *Compliance*-Maßnahmen dynamisch und automatisiert umsetzen kann.

9. AUTOREN

76



Michael Kranawetter besitzt durch sein BWL-Studium einen fundierten betriebswirtschaftlichen Hintergrund und nach 20 Jahren Erfahrung in der IT-Branche ein breites Wissen in den unterschiedlichsten Disziplinen der Informationsverarbeitung. Er realisierte unter anderem als Projektmanager und Berater erfolgreich große Infrastrukturprojekte, bevor er für eine große Rückversicherung in verschiedenen, internationalen Positionen als Projektmanager, Architekt, Chef Designer und Strategie in den Bereichen *Enterprise Architecture*, *Service Management* und *IT Governance* sowie *Directory Services* und Portal-Strategien tätig war. In den letzten drei Jahren trug er als Program Manager Risk Assessment die Verantwortung für das interne, global tätige Security Audit Team und war zudem für die Themen *Information Security Risk Management*, *Compliance* und *Governance* zuständig. Heute arbeitet er als National Security Officer für Microsoft. Hier ist er Ansprechpartner für Chief (Information) Security Officers, unter anderem für die Themen *Governance*, *Risk and Compliance* und für die Microsoft-Informationssicherheitsstrategie.



Martin Nuß ist als Teil des Microsoft Student Explorer Programs (STEP) im National Security Office von Microsoft Deutschland tätig. Die Schwerpunkte seiner Arbeit liegen auf den Themenkomplexen Informationssicherheit und *Compliance* mit besonderem Augenmerk auf *Cloud Computing* und Sicherheit in der digitalen Transformation. Im Rahmen seiner Arbeit setzt er sich sowohl mit strategisch-betriebswirtschaftlichen als auch mit technischen Fragestellungen auseinander. Bereits während seines Bachelorstudiums an der Universität Passau hat sich Herr Nuß vertiefend mit den Themen Informationssicherheit und *Cloud Computing* auseinandergesetzt. Zurzeit studiert er im Masterstudiengang Wirtschaftsinformatik im Schwerpunkt *IT Security* an der Universität Regensburg.



Dr.-Ing. Markus a Campo ist bei der ISG Germany als Senior Advisor tätig. Die Schwerpunkte seiner Arbeit liegen in der Informationssicherheit, speziell in der Analyse von IT-Architekturen und -Sicherheitskonzepten. Weitere Themen seiner Arbeit sind: Netzwerksicherheit allgemein, *Security Audits*, *Incident Response*, sicherer Einsatz von Smartphones, Sicherheit von Webapplikationen und Sicherheit von Zahlungssystemen sowie die Standards ISO 27001 und BSI-Grundschutzkataloge. Herr a Campo studierte Technische Informatik an der RWTH Aachen und promovierte dort 1991. Nach einer Anstellung in der IT-Abteilung eines Aluminiumkonzerns arbeitet er seit 1997 als Berater, Autor und Schulungsreferent mit dem Schwerpunkt Informationssicherheit. Er ist von der IHK Aachen öffentlich bestellter und vereidigter Sachverständiger mit dem Bestellungstenor „Systeme und Anwendungen der Informationsverarbeitung, insbesondere im Bereich IT-Sicherheit“. Weiterhin ist er zertifizierter ISO 27001 Lead Auditor sowie ISO 27001 Lead Implementer.

10. GLOSSAR

A

as a Service-Bereitstellung (*aaS)

Bedeutet, dass etwas in digitaler Form über das Internet durch einen Anbieter als Dienst bereitgestellt wird. Die *as a Service*-Bereitstellung grenzt sich von der eigenständigen *On-Premises*- bzw. *Inhouse*-Bereitstellung von Diensten auf Basis eigenständig bereitgestellter Ressourcen ab.

Advanced Persistent Threats (APT)

Beschreibt einen komplexen, zielgerichteten Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten. Ziele stellen in aller Regel Behörden sowie Groß- und Mittelstandsunternehmen dar.

Archivierung

Beschreibt die unveränderbare, langfristig angelegte Aufbewahrung elektronischer Informationen. Die Archivierung wird häufig durch spezielle Archivsysteme unterstützt, um die Langfristigkeit und Unveränderbarkeit der Aufbewahrung zu gewährleisten.

Auditierung und Zertifizierung

Auditierung beschreibt die (regelmäßige) Bewertung eines Unternehmensaspektes unter Anwendung bestimmter Audit-Vorgaben. Audits dienen der systematischen, unabhängigen und dokumentierten Untersuchung zur objektiven Feststellung der Qualität einer Dienstleistung. Werden bestimmte Anforderungen bzw. Standards erfüllt, so kann dies durch unabhängige Stellen zertifiziert werden. Zertifizierungen werden in aller Regel zeitlich befristet vergeben.

B

Big Data

Der Begriff *Big Data* beschreibt Datenmengen, die zu groß, komplex, schnelllebig oder zu schwach strukturiert sind, um sie mit herkömmlichen Methoden der Datenverarbeitung auszuwerten.

Bring Your Own Device (BYOD)

Bezeichnung für das Mitbringen privater mobiler Endgeräte in die Netzwerke von Unternehmen und Organisationen. Dies beinhaltet auch die Umsetzung von Organisationsrichtlinien, die den Zugriff auf Netzwerkressourcen reglementieren.

C

Cloud Computing

Als *Cloud Computing* wird gemeinhin die Bereitstellung skalierbarer IT-Ressourcen über das Internet durch einen Anbieter bezeichnet. *Cloud*-Dienste decken das gesamte Spektrum der IT ab und beinhalten unter anderem Infrastrukturdienste, Plattformdienste und Softwaredienste. Ein besonderes Erkennungsmerkmal stellt der Einsatz von Virtualisierungstechnologien dar. Deren Einsatz ermöglicht eine hohe Skalierbarkeit der Inanspruchnahme von Ressourcen durch *Cloud*-Kunden.

Cloud-Anbieter

Cloud-Anbieter bieten ihren Kunden *Cloud*-Dienste unterschiedlicher Art an. *Cloud*-Anbieter betreiben hierzu Datacenter, welche die notwendige Rechenkapazität und Infrastruktur zur Bereitstellung der *Cloud*-Dienste liefern. Basierend auf diesen Ressourcen können *Cloud*-Anbieter ihren Kunden Entwicklungsplattformen oder Rechenkapazität über virtuelle Maschinen bereitstellen, mit welchen *Cloud*-Kunden eigene Lösungen entwickeln können. Häufig betreiben *Cloud*-Anbieter auch eigene Softwaredienste in ihrer *Cloud* und stellen diese direkt über das Internet bereit.

Cloud-Dienstanbieter

Cloud-Dienstanbieter stellen ihren Kunden in der Regel Software- oder Plattformdienste (z. B. Entwicklungstools) zur Verfügung. In Abgrenzung zum *Cloud*-Anbieter stellen *Cloud*-Dienstanbieter die hierfür notwendige Datacenter-Infrastruktur nicht eigenständig bereit. *Cloud*-Dienstanbieter greifen hierfür auf Infrastrukturdienste anderer *Cloud*-Anbieter zurück.

Cloud-Kunde

Bei einem *Cloud*-Kunden handelt es sich um eine Organisation oder einen Endanwender, der einen oder mehrere *Cloud*-Dienste eines Anbieters in Anspruch nimmt und hierfür in der Regel ein von der Nutzung abhängiges Entgelt entrichtet.

Cloud-Lösungen

Analog zu einer Softwarelösung im Allgemeinen stellt eine *Cloud*-Lösung einen *Cloud*-Dienst dar, der eine bestimmte, z. B. betriebliche Anforderung umsetzt bzw. ein bestimmtes Problem löst.

Cloud-Dienstmodell

Cloud Computing wird häufig in drei unterschiedliche *Cloud*-Dienstmodelle unterteilt, welche unterschiedliche Arten von *Cloud*-Diensten sinnvoll kategorisieren. Hierbei werden häufig die drei geläufiger *Cloud*-Dienstmodelle genannt: *Software as a Service (SaaS)* beschreibt die Bereitstellung von kompletten Softwareapplikationen über das Internet. *Platform as a Service (PaaS)* stellt die Bereitstellung von Entwicklungsumgebungen über das Internet dar, die zur Entwicklung eigener Softwareanwendungen herangezogen werden können. *Infrastructure as a Service (IaaS)* bedeutet, dass virtualisierte Rechenressourcen wie Rechenzeit, Speicherkapazität o. Ä. über das Internet bereitgestellt werden.

Cloud-Technologie

Eine Reihe neuer Geschäftsmodelle sowie technologischer Innovationen basiert auf *Cloud Computing*. Diese werden im Rahmen dieses Werkes als *Cloud*-Technologien bezeichnet.

Compliance, IT Compliance, Corporate Compliance

IT Compliance beschäftigt sich als Teilbereich der *Compliance* schwerpunktmäßig mit denjenigen *Compliance*-Anforderungen, welche die IT-Systeme eines Unternehmens oder einer Organisation betreffen. Der Begriff *Corporate Compliance* soll im Rahmen dieses Handbuchs zur Abgrenzung von der *IT Compliance* dienen. Mit *Corporate Compliance* sind also diejenigen *Compliance*-Anforderungen gemeint, welche vom Begriff der *IT Compliance* nicht erfasst werden. Wird der allgemeine *Compliance*-Begriff verwendet, so ist sowohl IT, als auch *Corporate Compliance* gemeint.

Compliance-Anforderung

Eine *Compliance*-Anforderung stellt eine konkrete Voraussetzung dar, welche zur Einhaltung einer bestimmten regulatorischen, internen oder vertraglichen Vorgabe notwendigerweise erfüllt werden muss. In der Regel leiten sich *Compliance*-Anforderungen aus gesetzlichen Regularien, internen Vorschriften oder dem Inhalt von Verträgen ab.

Compliance-Handlungsfelder

Handlungsfelder stellen im Kontext des *Compliance*-Modells konkrete Ausprägungen der Kernbereiche regulatorischer und geschäftlicher Anforderungen dar, die eine bestimmte *Compliance*-Thematik erfassen und abdecken. Es handelt sich also um thematisch abgegrenzte Kategorien von *Compliance*-Anforderungen, die durch bestimmte Maßnahmen, Prozesse und *Workflows* berücksichtigt werden können.

Compliance-Kernbereiche

Kernbereiche stellen Kategorien im Kontext des *Compliance*-Modells dar, die sich aus den gemeinsamen Zielen regulatorischer und geschäftlicher Anforderungen ergeben. Die sechs Kernbereiche orientieren sich dabei an gängigen Organisationsstrukturen und Verantwortlichkeiten.

Compliance-Modell

In diesem Handbuch wird ein *Compliance*-Modell beschrieben, das die gemeinsamen Ziele regulatorischer und geschäftlicher Anforderungen abbildet. Diese Ziele werden in Kernbereichen und Handlungsfeldern zusammengefasst und aufgegriffen. Das Modell kann als Verständnismodell zur strukturierten Abbildung der Thematik sowie als Anwendungsmodell für die Erstellung eines generischen Abbilds auf Basis weiterführender Analysen herangezogen werden.

Compliance-Prozesse

Um *Compliance*-Anforderungen umzusetzen und um diese Umsetzung sicherzustellen, wenden Unternehmen vermehrt Prozesse an, also standardisierte Abläufe. *Compliance*-Prozesse bilden etwa spezifische *Compliance*-Anforderungen in Geschäftsprozessen ab oder beschreiben Maßnahmen, welche die Umsetzung von *Compliance*-Maßnahmen überprüfen.

Compliance-Risiken

Compliance-Risiken entstehen, wenn Organisationen durch Verstöße gegen Regularien, Verträge oder interne Vorgaben Gefahr laufen, Schäden zu erleiden. Häufige Folgen von *Compliance*-Verstößen sind etwa rechtliche Sanktionen, finanzielle Verluste oder Schäden an der Unternehmensreputation.

D

Datenschutz

Maßnahmen, welche die Daten von Individuen bei der Verarbeitung durch Dritte betreffen. Beinhaltet den Schutz vor der Beeinträchtigung des Rechtes auf informationelle Selbstbestimmung einer Person. Demnach darf jeder Bürger grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden.

Digitale Transformation

Der Begriff „digitale Transformation“ beschreibt einen fortlaufenden, in digitalen Technologien begründeten Veränderungsprozess. Dieser betrifft die gesamte Gesellschaft und wirkt sich in besonderem Maße auf die strategische Ausrichtung, Innovationen und Innovationszyklen sowie die IT-Prozessunterstützung in Unternehmen und Organisationen aus.

Dynamik

Im Kontext des *Compliance*-Modells bezeichnet der Begriff Dynamik ein gemeinsames Ziel regulatorischer und geschäftlicher Anforderungen, das auf eine hohe Adaptierbarkeit technologischer und organisatorischer Merkmale in Organisationen und Unternehmen abzielt. Hintergrund ist die Schnelllebigkeit der Entwicklungen und Trends der IT im Zuge der digitalen Transformation.

F

Funktionstrennung (engl. *segregation of duties*)

Der Begriff Funktionstrennung beschreibt die organisatorische Trennung zwischen Organisationseinheiten, die an bestimmten Geschäftsprozessen beteiligt sind. Dient der Vermeidung von Interessenskonflikten.

G

Governance, Risk Management and Compliance (GRC)

Fasst drei elementar wichtige Handlungsebenen einer erfolgreichen Unternehmensführung zusammen.

- *Governance* bezeichnet im Allgemeinen den Aufbau eines Steuerungs- und Regelungssystems in einer Organisation im strukturellen Sinne. Beinhaltet die Definition von Richtlinien und die Festlegung von Unternehmenszielen.
- *Risk Management* beschreibt den Umgang mit bekannten und unbekannten Risiken basierend auf Risikoanalysen. Beinhaltet frühzeitige Auseinandersetzung und die Erarbeitung von Strategien zur Risikominimierung sowie Vorbereitungen auf den Risikoeintritt.
- *Compliance* beschreibt das Einhalten interner und externer Normen (vgl. Begriffserklärungen zu *Compliance*, *IT Compliance*, *Corporate Compliance* im Glossar).

I

Identitäts- und Zugriffsmanagement (IAM)

IAM (Abkürzung aus dem Englischen: *Identity and Access Management*) umfasst das Verwalten von Benutzeridentitäten und deren Zugangsberechtigungen zu allen Systemen, Daten und Informationen einer Organisation.

Individualisierung

Der Begriff Individualisierung wird in diesem Handbuch im ökonomischen Kontext der Individualisierung von Produkten und Dienstleistungen verwendet. Durch das Internet werden mehr und mehr Prozesse ermöglicht, mit denen sich Kunden durch das Einbringen persönlicher Anforderungen am Gestaltungsprozess von Produkten und Dienstleistungen beteiligen können.

Informationssicherheit und -schutz

Eigenschaft von IT-Systemen, die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit einzuhalten, um Risiken zu minimieren und wirtschaftliche Schäden zu vermeiden.

Interface

Der Begriff *Interface* (dt. Schnittstelle) beschreibt den Teil eines IT-Systems, welcher der Kommunikation mit anderen Systemen, Benutzern oder Prozessen dient.

Internet der Dinge (IoT, *Internet of Things*)

Der Begriff „Internet der Dinge“ impliziert den Trend, dass zunehmend „intelligente Gegenstände“ (z. B. eingebettete Systeme in Industriemaschinen, Autos o. Ä.) an Netzwerke angeschlossen werden, um automatisiert Informationen auszutauschen oder bereitzustellen.

IT-Infrastruktur

Der Begriff IT-Infrastruktur bezeichnet im allgemeinen IT-Kontext alle Komponenten, die zum Betrieb von Softwareapplikationen benötigt werden. Der Begriff umfasst dabei sowohl Hardwarekomponenten als auch grundlegende Softwarekomponenten. Im *Cloud*-Kontext zählen hierzu zum Beispiel Softwarekomponenten zur Bereitstellung der Virtualisierung.

K

Künstliche Intelligenz (KI)

Künstliche Intelligenz soll durch Methoden ermöglicht werden, die es einem Computersystem ermöglichen, auf Basis von Algorithmen automatisiert Problemlösungen zu entwickeln.

M

Malware

Malware (dt. Schadprogramme) sind Computerprogramme, die mit dem Ziel entwickelt wurden, unerwünschte und schädliche Funktionen auszuführen.

Managed Security Services (MSS)

Externe Dienstleistungen, mit denen allgemeine oder Teilaspekte der Netzwerk- und IT-Sicherheit in Unternehmen und Organisationen verwaltet bzw. abgedeckt werden können.

Maschinelles Lernen

Beschreibt das Erlernen von Wissen aus Erfahrung durch ein System. Dieses lernt aus Beispielen und kann diese anschließend durch die Erkennung von Mustern und Gesetzmäßigkeiten verallgemeinern.

Mehr-Augen-Prinzip

Das Mehr-Augen-Prinzip besagt, dass wichtige Tätigkeiten oder kritische Entscheidungen nicht von einer einzelnen Person, sondern von mehreren Personen ausgeführt werden müssen. Ziel ist die Fehlervermeidung und die Reduzierung der Gefahr von Missbrauch.

Mobile Computing/Mobile Workspace

Mobile Computing umfasst alle Technologien und Elemente, die notwendig sind, um einen *Mobile Workspace* bereitzustellen. Hierzu gehören etwa mobile Hardware, Netzwerkanbindungen, mobil verfügbare *Cloud*-Speicher etc. Der *Mobile Workspace* stellt Nutzern eine ortsunabhängig einsetzbare Arbeitsumgebung bereit, die Zugänge zu Applikationen, Daten und Diensten beinhaltet.

N

Nutzenpotenziale/Synergien

Nutzenpotenziale oder Synergieeffekte werden erzielt, wenn durch das Zusammenwirken von Einzelkräften zu einer Gesamtleistung ein höherer Nutzen erzielt wird als bei der Summe derselben Einzelleistungen. Im Kontext dieses Handbuchs werden beide Begriffe dazu verwendet, um die Steigerung des Gesamtnutzens in Organisationen durch die gemeinsame Betrachtung sich überschneidender geschäftlicher und regulatorischer Anforderungen zu beschreiben.

O

On-Premises-/Inhouse-Software

On-Premises-Software oder *Inhouse*-Software beschreibt ein Nutzungs- und Lizenzmodell für serverbasierte Software. Ein Lizenznehmer mietet Software, betreibt sie allerdings im eigenen Rechenzentrum oder mietet Server hierfür an.

Organisationsstruktur

Eine Organisationsstruktur bildet ein System von Kompetenzen ab, das den Handlungsrahmen der arbeitsteiligen Aufgabenerfüllung in Organisationen festlegt.

P

Perimeter

Im Kontext der IT-Sicherheit stellt ein Perimeter ein abgegrenztes Privat- oder Organisationsnetz dar, das durch Schnittstellen mit der Außenwelt verbunden ist. Die Perimetersicherheit betrifft somit den strategischen Schutz vor Angriffen, die den Datenverkehr mit öffentlichen Netzen über diese Schnittstellen ausnutzen.

Personenbezogene Daten

Der Begriff entstammt dem Datenschutzrecht. Daten sind personenbezogen, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet werden können.

Phishing

Phishing beschreibt Betrugsversuche, die darauf abzielen, Internetnutzer mit Hilfe gefälschter Webseiten, E-Mails oder Nachrichten zur Preisgabe persönlicher Informationen (z. B. Passwörtern, Kontonummern etc.) zu verleiten.

Prinzip der Mindestinformation (Need-to-know-Prinzip)

Sicherheitsziel, das die Beschränkung des Zugriffs auf Daten und Informationen einer Sicherheitsebene durch Personen auf solche Informationen vorsieht, die unbedingt für die Erfüllung einer konkreten Aufgabe notwendig sind.

R

Reifegradmodell

Strukturelle Zusammenstellung sogenannter Reifegradstufen, welche die Wirksamkeit und Nachhaltigkeit von Prozessen beschreiben. Ein Reifegradmodell bietet einen Ausgangspunkt für mögliche Prozessverbesserungen und etabliert eine gemeinsame Sprache bei der Bewertung von Prozessen.

Risikomanagement

Risikomanagement umfasst sämtliche Maßnahmen, die den Umgang mit Risiken festlegen. Dazu gehören Erkennung, Analyse, Bewertung, Überwachung und Kontrolle von Risiken.

Repository

Ein *Repository* (englisch für Lager, Depot oder auch Quelle) ist ein verwaltetes Verzeichnis zur Speicherung und Beschreibung von digitalen Objekten für ein digitales Archiv.

S

Schutzbedarfsanalyse

Die Schutzbedarfsanalyse dient der Identifikation sensibler Güter (z. B. Daten) und der Erkennung potenzieller Bedrohungen für diese. Dazu gehören auch die Abwägung potenzieller Schäden und Risiken sowie die Ableitung von Schutzmaßnahmen.

Schwachstellenmanagement

Schwachstellenmanagement beschreibt die systematische und fortlaufende Überprüfung, Erkennung und Behebung von Sicherheitslücken in IT-Systemen (z. B. Software und Netzwerke).

Service Level Agreement (SLA)

Eine Vereinbarung zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen, in der vom Dienstleister zugesicherte Leistungseigenschaften genau spezifiziert werden. Ziel ist es, die Kontrollmöglichkeiten des Auftraggebers transparent darzulegen.

Single Sign-on (SSO)

SSO bedeutet, dass ein Benutzer durch eine einmalige Authentifizierung an einem Arbeitsplatz ohne Neuanmeldung Zugriff auf alle Rechner und Dienste erhält, die seine Berechtigung vorsieht.

Skalierbarkeit

Im Kontext von IT-Systemen stellt Skalierbarkeit die Fähigkeit dar, die Leistung durch das Hinzufügen oder Entfernen von Ressourcen (z. B. Hardware) innerhalb definierter Schranken anpassen zu können.

Social Engineering

Social Engineering umfasst verschiedene Methoden der betrügerischen zwischenmenschlichen Einflussnahme, die das Ziel verfolgen, bei einem Opfer bestimmte Verhaltensweisen hervorzurufen. Hierzu gehört häufig die Preisgabe vertraulicher Informationen oder die Freigabe von Finanzmitteln. *Social Engineers* spionieren das persönliche Umfeld ihrer Zielperson aus, täuschen Identitäten vor oder nutzen bestimmte Verhaltensweisen aus, um ihr Ziel zu erreichen.

Sorgfaltspflicht

Sorgfaltspflichten leiten sich im Unternehmensumfeld aus unterschiedlichen regulatorischen Anforderungen her und beschreiben beispielsweise Anforderungen an die Unternehmensführung und Buchführung.

T

Technologiemanagement

Der Begriff Technologiemanagement beschreibt die Planung, Durchführung und Kontrolle der Entwicklung und Anwendung von (neuen) Technologien. Der Einsatz von Technologien dient dem Erzeugen erfolgswirksamer Wettbewerbsvorteile.

Transparenz

Transparenz beschreibt die Eigenschaft einer Person oder Organisation, der Öffentlichkeit oder einem bestimmten Interessentenkreis freien Zugang zu Informationen zu gewähren und stetige Rechenschaft über bestimmte Abläufe, Sachverhalte und Vorhaben zu liefern. Im Kontext von *Compliance* in Organisationen stellt Transparenz eine wichtige Voraussetzung dar, um öffentlichen Stakeholdern nachvollziehbare Informationen über die Einhaltung von Regularien und Verträgen zu übermitteln.

Trojaner

Als Trojaner wird im Kontext der IT-Sicherheit ein Schadprogramm bezeichnet, das als nützliches Programm getarnt ist. Führt ein Nutzer ein solches Programm aus, führt ein Trojaner neben oder anstatt seiner vorgetäuschten Funktion im Hintergrund andere, schädliche Funktionen aus.

V

Verfügbarkeit

Schutzziel, welches das Maß der Erreichbarkeit bzw. Verwendbarkeit von Daten oder IT-Systemen innerhalb eines bestimmten zeitlichen Rahmens bemisst. Eine Verletzung dieses Schutzziels kann z. B. aus menschlichem Versagen, gezielten Angriffen oder technischen Störungen resultieren.

Verständnismodell, Anwendungsmodell

Im Kontext dieses Handbuchs beschreibt der Begriff Verständnismodell ein Modell, das zur Veranschaulichung und vereinfachten Darstellung eines Sachverhalts verwendet werden kann. In Abgrenzung hierzu beschreibt der Begriff Anwendungsmodell ein Modell, das zur Umsetzung konkreter Handlungen (z. B. Analysen und Beurteilungen) herangezogen werden kann.

Virtualisierung

Technologie, die es ermöglicht, IT-Ressourcen mit Hilfe einer Abstraktionsschicht nachzubilden. So lassen sich nicht-physische Geräte wie emulierte Hardware, Betriebssysteme oder Datenspeicher erzeugen. Diese können transparent zusammengefasst und von mehreren Nutzern verwendet werden. Im *Cloud*-Kontext ermöglicht die Virtualisierung etwa die Skalierbarkeit von IT-Ressourcen und die Trennung mehrerer Mandanten in einer einzelnen Serverumgebung.

W

Workflows und Geschäftsprozesse

Bei einem Geschäftsprozess handelt es sich um eine Menge logisch verknüpfter Einzeltätigkeiten, die zur Erreichung eines bestimmten betrieblichen oder geschäftlichen Ziels ausgeführt werden. Ein *Workflow* stellt eine detaillierte Beschreibung von Einzeltätigkeiten dar, die in Systemen abgebildet werden können. So können Geschäftsprozesse unterstützt und ggf. (teil-)automatisiert werden.

11. ANALYSTENFAZITS – ISG GROUP

11.1 Über ISG



ISG (Information Services Group, (NASDAQ: ILL)) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologiesegment. Als zuverlässiger Geschäftspartner für über 700 Kunden, darunter 75 der 100 weltweit größten Unternehmen, unterstützt ISG Unternehmen, öffentliche Organisationen sowie Service- und Technologieanbieter dabei, Operational Excellence und schnelleres Wachstum zu erzielen. Der Fokus des Unternehmens liegt auf Services im Kontext der digitalen Transformation, inklusive Automatisierung, Cloud und Datenanalytik, des Weiteren auf Sourcing-Beratung, Managed Governance und Risk Services, Services für den Netzbetrieb, Design von Technologiestrategie und -betrieb, Change Management sowie Marktforschung und Analysen in den Bereichen neuer Technologien. 2006 gegründet, beschäftigt ISG mit Sitz in Stamford, Connecticut, über 1.300 Experten und ist in mehr als 20 Ländern tätig. Das globale Team von ISG ist bekannt für sein innovatives Denken, seine geschätzte Stimme im Markt, tiefgehende Branchen- und Technologieexpertise sowie weltweit führende Marktforschungs- und Analyseressourcen, die auf den umfangreichsten Marktdaten der Branche basieren.

© 2017 Information Services Group, Inc. Alle Rechte vorbehalten.

Mehr Informationen zu unserem Research finden sie unter: <http://isg-one.com/research>

11.2 Analystenfazits

Die digitale Transformation stellt neue Herausforderungen an die Erfüllung von *Compliance*-Anforderungen. Diese waren Anlass für die Weiterentwicklung des *Compliance*-Modells.

Mit dem *Compliance*-Modell kann der aktuelle Status der eigenen *Compliance* einfach und anschaulich ermittelt werden. Zudem werden Potenziale für Verbesserungen sichtbar.

Nutzníeßer der digitalen Transformation sind Unternehmer, deren Mitarbeiter sowie die Kunden.

Im Zuge der digitalen Transformation werden *Workflows* standardisiert und automatisiert. Dadurch werden Fehler vermieden, Angriffe verhindert und Geschäftsprozesse optimiert.

Die Anforderungen der digitalen Transformation an *Workflows*, Arbeitsplätze und -techniken lassen sich durch den verstärkten Einsatz von *Cloud*-Technologien erfüllen. Das Internet der Dinge ist ohne *Cloud* sogar undenkbar.

Mit der digitalen Transformation entstehen neue Herausforderungen für die *Compliance*. Diese können mit Hilfe von technischen Lösungen, Regularien und Standards umgesetzt werden.

Umsetzbarkeit und Erfolg der digitalen Transformation stehen und fallen mit der fortlaufenden Umsetzung regulatorischer Anforderungen. Die *Cloud* stellt hierfür eine Basistechnologie dar, da sie für den Informationsaustausch innerhalb der *Workflows* erforderlich ist und sich mit ihrer Hilfe viele *Compliance*-Anforderungen erfüllen lassen.

Im Zuge der digitalen Transformation werden die Bereiche der *Compliance*, die noch ohne IT auskommen, immer kleiner werden. Die IT unterstützt zunehmend Geschäftsprozesse und *Compliance*-Lösungen, die bisher keinen oder nur einen minimalen Anteil an IT hatten.

Ein *Cloud*-Anbieter muss sich mit den Themen Sicherheit, *IT Compliance* und Transparenz beschäftigen. *Compliance* stellt mitnichten nur eine kostspielige, aber strategisch irrelevante Notwendigkeit dar. Die Umsetzung von *Compliance*-Anforderungen wird immer auch einen Beitrag zur Steigerung des Geschäftserfolges leisten.

Neue IT-Technologien ermöglichen die Gestaltung von Prozessen, mit denen die Einhaltung von *Compliance*-Anforderungen sichergestellt und überwacht wird, auch in Bereichen, in denen bisher keine oder kaum IT zum Einsatz kam.

Mittels IT-Technologien lassen sich entscheidende Bereiche von *Governance*, *Risk Management* und *Compliance* automatisiert umsetzen. Das dient nicht nur der Erfüllung von Anforderungen, sondern hat einen praktischen Nutzen für die eigene Organisation.

Regulatorische und geschäftliche Anforderungen beruhen auf gemeinsamen Intentionen. Diese lassen sich über die sechs Ziele Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz, Sorgfalt und Dynamik formulieren und in die Tat umsetzen.

Das *Compliance*-Modell ist dreistufig aufgebaut. Aus allgemeinen Zielen ergeben sich Kernbereiche von Aktivitäten, die schließlich über Prozesse und *Workflows* in bestimmten Handlungsfeldern umgesetzt werden.

Mit dem *Compliance*-Modell lässt sich eine qualitative Messung des Reifegrades von *Compliance*-Prozessen durchführen. Daraus lassen sich Verbesserungspotenziale ableiten, mit denen der Reifegrad weiter gesteigert wird.

ABBILDUNGSVERZEICHNIS

- Abbildung 1:** Zusammenfassung des *Compliance*-Modells
- Abbildung 2:** Verteilung Expertengespräche
- Abbildung 3:** Bedeutung der Digitalisierung für Unternehmen
- Abbildung 4:** Bedeutung von Technologien für die digitale Transformation
- Abbildung 5:** Aufgaben *Compliance*-Verantwortliche
- Abbildung 6:** *Compliance*-Bedeutung für Mitarbeiter
- Abbildung 7:** *Microsoft Insights Studie* – Bedeutung von Cyberbedrohungen
- Abbildung 8:** *Microsoft Insights Studie* – Nutzung von *Cloud Computing*
- Abbildung 9:** *Microsoft Insights Studie* – Bedeutung von Qualitäten eines *Cloud*-Anbieters
- Abbildung 10:** *Cloud* und digitale Transformation
- Abbildung 11:** Digitalisierung von *Workflows*
- Abbildung 12:** Expertenmeinung – Bedeutung von Standardisierung und Automatisierung für *Compliance*
- Abbildung 13:** *Compliance*-Modell – Gemeinsame Ziele regulatorischer und geschäftlicher Anforderungen
- Abbildung 14:** *Compliance*-Modell – Kernbereiche regulatorischer und geschäftlicher Anforderungen
- Abbildung 15:** *Compliance*-Modell – Motivation exemplarischer Handlungsfelder
- Abbildung 16:** *CMMI*-Reifegradmodell
- Abbildung 17:** Beschreibung der *CMMI*-Reifegradstufen
- Abbildung 18:** Prozessreife und Prozesskosten
- Abbildung 19:** *KPMG Self-Assessment* – Grafische Darstellung der Analyseergebnisse (Beispiel)
- Abbildung 20:** Aufteilung der Zuständigkeiten zwischen *Cloud*-Anbieter und -Kunde

COPYRIGHT

Dieses Dokument dient lediglich der Information. MICROSOFT ÜBERNIMMT KEINE HAFTUNG FÜR DIE IM DOKUMENT ENTHALTENEN INFORMATIONEN, UNGEACHTET OB EXPLIZIT, IMPLIZIT ODER VOM GESETZ VORGESCHRIEBEN.

Microsoft ist unter Umständen im Besitz von Patenten, Patentanmeldungen, Warenzeichen, Copyrights oder sonstigem Anspruch auf geistiges Eigentum hinsichtlich der Inhalte des vorliegenden Dokuments. Außer im Fall einer ausdrücklichen Lizenzvereinbarung mit Microsoft berechtigt Sie die Bereitstellung des Dokuments nicht zur Nutzung dieser Patente, Warenzeichen, Copyrights oder sonstigen Ansprüche.

© 2017 Microsoft Corporation. Alle Rechte vorbehalten.

© 2017 ISG Germany GmbH bezogen auf ISG Grafiken. Die Schlussfolgerungen über Ansichten von Entscheidern des deutschen Marktes basieren auf den Ergebnissen einer Umfrage der ISG Germany GmbH und obliegen der ISG Germany GmbH. Trotz der gewissenhaften und mit größter Sorgfalt ermittelten Informationen und Daten kann für deren Vollständigkeit und Richtigkeit keine Garantie übernommen werden. Alle Rechte am Inhalt dieser Umfrage liegen bei der ISG Germany GmbH.

Die Daten und Informationen bleiben aus Gründen des Datenschutzes Eigentum der ISG Germany GmbH.

Vervielfältigungen, auch auszugsweise, bedürfen des Quellenhinweises.

Weitere Informationen unter:

<https://servicetrust.microsoft.com>

<https://www.microsoft.com/de-de/trustcenter>

<https://www.microsoft.com/de-de/cloud-platform>

<http://isg-one.com/research>