

Inhaltsverzeichnis

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

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

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

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

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