

Inhaltsverzeichnis

Abbildungsverzeichnis.....	IX
Tabellenverzeichnis	XI
1 Einführung – Warum Metriken?	1
2 Metrik – Definition und Begriffsabgrenzung	3
2.1 Metrik: Definition und Kategorisierung.....	4
2.1.1 Sicherheitsmetriken.....	5
2.1.2 Softwaremetriken	7
2.2 Metriken für Security und Compliance.....	8
2.2.1 Metriken und IT-Governance	9
2.2.2 Security Compliance Metriken – Definition	11
2.2.3 Operative Metriken	15
2.2.4 Incident Management Metrics.....	18
2.2.5 Verwandte und ergänzende Metriken	20
3 Monitoring, Metriken und IT-Kontrollen	21
3.1 Auswahl wesentlicher Kontrollen in der IT.....	22
3.1.1 Ansätze zu Ableitung wesentlicher Kontrollen	22
3.1.2 Merkmale wesentlicher Kontrollen.....	23
3.1.3 Klassifizierung nach Public Company Accounting Board (PCAOB).....	25
3.1.4 Klassifizierung nach Debra S. Herrmann.....	25
3.1.5 Klassifizierung nach ISO/IEC 27002	26
3.1.6 Klassifizierung nach COBIT 4.1.....	27
3.2 Monitoring versus Audit.....	29
4 Metriken im Universum regulatorischer Anforderungen	31
4.1 Sarbanes-Oxley Act (SOX).....	34
4.2 Bilanzrechtsmodernisierungsgesetz (BilMoG).....	35
4.3 Bundesdatenschutzgesetz (BDSG).....	35
4.4 Kreditwesengesetz (KWG).....	37
4.5 Standards.....	39
4.5.1 Standards der ISO und des BSI für Informationssicherheits- und Risikomanagement.....	41
4.5.2 Control Objectives for Information and Related Technology (COBIT).....	43
4.5.3 Standards und Grundsätze des IDW.....	44

5	Methodik zur Entwicklung effektiver Metriken	49
5.1	Goal-Question-Metrics (GQM)	50
5.2	Datenerhebung und Messungen (Measurements)	52
5.2.1	Entwicklung eines „Messplans“	54
5.2.2	Qualität der Daten	55
5.2.3	Quantität der Daten	57
5.2.4	Sammlung von Daten	58
5.2.5	Validierung der Daten und Datenintegrität	59
5.2.6	Archivierung und Ablage der Daten	60
5.2.7	Analyse und Interpretation von Daten	61
6	Lebenszyklus einer Metrik	65
6.1	Prozess zur Implementierung des Monitoring	65
6.2	Verfahren zur Gestaltung von IT-Kontrollen	67
6.3	Verfahren zur Gestaltung und Aktualisierung von Metriken	70
6.3.1	Teilprozess zum routinemäßigen Einsatz von Metriken (B)	70
6.3.2	Teilprozess zur Gestaltung und Aktualisierung von Metriken (A)	71
6.4	Festlegen der <i>control baseline</i> und der Schwellenwerte	76
6.5	Effiziente Metriken	77
6.6	Effektive Metriken	80
7	Aggregation von Metriken für verschiedene Zielgruppen	83
7.1	Internes Reporting	83
7.1.1	Adressaten des Reporting	84
7.1.2	Arten des Reporting	88
7.1.3	Frequenz des Reporting	90
7.1.4	IT-relevante Inhalte in den Reports	92
7.2	Externes Reporting	97
7.3	Benchmark	100
7.3.1	Bestimmung der IT-Compliance Reife mit COBIT	102
8	Darstellung der Metrik-Resultate	107
8.1	Graphische Darstellungen der Resultate	107
8.2	Darstellung aggregierter Metrik-Resultate	109
9	Fazit und Ausblick	113
10	Metrik-Sammlung	115
	Literatur	131
	Sachwortverzeichnis	135