

Inhaltsverzeichnis

1	Einleitung	1
	Literatur	4
2	Grundlagen zur Zertifizierung von Cloud-Services	5
2.1	Cloud-Computing	5
2.1.1	Charakteristiken	6
2.1.2	Service-Modelle	7
2.1.3	Bereitstellungsmodelle	10
2.1.4	Risiken beim Einsatz von Cloud-Services	12
2.2	Zertifizierung von Cloud-Services	17
2.2.1	Nutzen von Zertifizierungen für Cloud-Service-Anbieter	18
2.2.2	Nutzen von Zertifizierungen für Cloud-Service-Kunden	19
2.2.3	Marktübersicht über Cloud-Service-Zertifizierungen	20
	Literatur	24
3	Gestaltungsempfehlungen für Cloud-Service-Zertifizierungen	29
3.1	Wahrnehmung von Cloud-Service-Zertifizierungen	29
3.2	Gestaltungsempfehlungen für Cloud-Service-Zertifizierungen	30
3.3	Gestaltungsempfehlungen für informative Kriterienkataloge und Prüfberichte	34
4	Kriterienkatalog zur Zertifizierung von Cloud-Services	43
4.1	Zugrundeliegende Struktur des Kriterienkatalogs	43
4.2	Kriterienkatalog	46
4.2.1	Verfügbarkeits- und Kapazitätsmanagement	47
4.2.2	Sicherheitsarchitektur	49

4.2.3	Berechtigungskonzept	52
4.2.4	Datenmanagement	55
4.2.5	Verschlüsselung	57
4.2.6	Virtualisierung	60
4.2.7	Sicherheitsmanagement	61
4.2.8	Netzwerkmanagement	63
4.2.9	Infrastrukturmanagement	64
4.2.10	Compliance-Management	66
4.2.11	Incident-Management	69
4.2.12	Risikomanagement	71
4.2.13	Notfallmanagement	72
4.2.14	Änderungs- und Release-Management	74
4.2.15	Fremddienstleistungen	76
4.2.16	Entwicklungsprozess	78
4.2.17	Administration	79
4.2.18	Prozessmanagement	80
4.2.19	Mitarbeitermanagement	81
4.2.20	Vertragsmanagement	82
4.2.21	Kundenmanagement	88
	Literatur	90
5	Kontinuierliche Zertifizierungsverfahren	93
5.1	Probleme bestehender Zertifizierungsprozesse	94
5.1.1	Ablauf eines Zertifizierungsprozesses	94
5.1.2	Probleme bei traditionellen Zertifizierungsprozessen	95
5.2	Automatisierung von Zertifizierungsprozessen zur Schaffung von Vertrauen und Transparenz	97
5.2.1	Datenerhebung	99
5.2.2	Datenübermittlung	101
5.2.3	Datenanalyse	102
5.2.4	Zertifikatsausstellung	102
5.2.5	Prozessanpassung	103
5.3	Umfang einer kontinuierlichen Zertifizierung	104
5.3.1	Richtlinien zur Bewertung des Erfordernisses einer kontinuierlichen Prüfung	104
5.3.2	Entscheidungsregeln für die Machbarkeit von automatisierten Überprüfungen	108
5.3.3	Exemplarische Anforderungsbereiche	113

5.4	Verändertes Wertschöpfungsnetzwerk einer kontinuierlichen Zertifizierung	117
	Literatur	123
6	Anforderungen und Rahmenbedingungen von kontinuierlichen Zertifizierungen	129
6.1	Anforderungen und Handlungsempfehlungen zur Durchführung von kontinuierlichen Zertifizierungen	129
6.1.1	Rechtliche Anforderungen	130
6.1.2	Technische Anforderungen	132
6.1.3	Organisatorische Anforderungen	134
6.1.4	Inhaltliche Anforderungen bezogen auf den Kriterienkatalog	135
6.2	Grenzen einer kontinuierlichen Zertifizierung	136
6.3	Risiken einer kontinuierlichen Zertifizierung	140
	Literatur	145
7	Messverfahren zur Durchführung von kontinuierlichen Zertifizierungen	147
7.1	Messverfahren zur Durchführung einer kontinuierlichen Zertifizierung	147
7.1.1	Verfahren zum Monitoring von Cloud-Services	148
7.1.2	Verfahren zur Auditierung von Cloud-Services	153
7.2	Metriken zur Messung von Cloud-Service-Eigenschaften	161
7.2.1	Metriken zur Messung von Cloud-Service-Kennzahlen	161
7.2.2	Metriken zur Bestimmung des Sicherheitsniveaus	170
7.3	Regelwerk zur Identifizierung von Verstößen und Initiierung von Maßnahmen	175
7.3.1	Feststellung der Nicht-Erfüllung von Zertifizierungskriterien	176
7.3.2	Bewertung	177
7.3.3	Initiierung von Maßnahmen	178
	Literatur	181
8	Monitoring-basiertes Zertifizierungsverfahren	189
8.1	Monitoring-basierte Messverfahren zur Durchführung einer kontinuierlichen Zertifizierung	189
8.2	Anforderungen an Monitoring-Systeme für die kontinuierliche Zertifizierung	192
8.2.1	Ressourcen-Schicht: Erhebung von Monitoring-Daten ...	192

8.2.2	Monitoring-Server: Verarbeitung von Daten	194
8.2.3	Datenbank: Speicherung und Verwaltung von Daten	195
8.2.4	Interface: Bereitstellung von Daten	196
8.2.5	Nicht-funktionale Anforderungen	197
8.3	Richtlinien zum Design von Monitoring-Systemen für die kontinuierliche Zertifizierung	199
8.3.1	Nutzung vorhandener Überwachungstechnologien zur Erfassung zertifizierungsrelevanter Daten	199
8.3.2	Anwenden eines agenten-basierten Architekturmodells	205
8.3.3	Flexible Datenspeicher einbinden und Daten sicher verwalten	208
8.3.4	Sicherer Datenaustausch	211
8.4	Prototypische Entwicklung eines Monitoring-Systems für die kontinuierliche Zertifizierung	214
8.4.1	Komponenten des Prototypens	214
8.4.2	Prozessablauf	216
8.4.3	Evaluierung des Prototyps	217
	Literatur	219
9	Marktpotenzial einer kontinuierlichen Zertifizierung	223
9.1	Akzeptanz einer kontinuierlichen Zertifizierung durch Cloud-Service-Anbieter und Zertifizierungsstellen	223
9.1.1	Relativer Vorteil	225
9.1.2	Kompatibilität	227
9.1.3	Komplexität	229
9.1.4	Erprobbarkeit	230
9.1.5	Beobachtbarkeit	231
9.2	Gestaltungsempfehlungen zur Realisierung von Vorteilen und Potenzialen für Cloud-Service-Kunden	232
9.2.1	Vorteile für Cloud-Service-Kunden durch eine kontinuierliche Zertifizierung	232
9.2.2	Gestaltungsempfehlungen zur Realisierung der Vorteile für Cloud-Service-Kunden	234
	Literatur	237
10	Fazit & Ausblick	239
	Literatur	242

11 Anhang: Vorgehensweise	243
11.1 Entwicklung einer Taxonomie für Cloud-Service- Zertifizierungskriterien	244
11.2 Klassifizierung der Zertifizierungskriterien	247
11.3 Workshops zur Schärfung der Ergebnisse	248
Literatur	249