
Inhaltsverzeichnis

- I **Die Enttarnung der Cloud** 1
 - 1.1 Entstehung des MEGA-Trends 7
 - 1.2 Basistechnologien und Konzepte 10
 - 1.2.1 Konsolidierung und Virtualisierung 10
 - 1.2.2 Service-orientierte Architekturen 11
 - 1.2.3 Grid-Computing 12
 - 1.2.4 Utility-Computing 12
 - 1.2.5 Application Service Providing 13
 - 1.3 Merkmale von Cloud-Services 13
 - 1.3.1 On Demand Self Service 13
 - 1.3.2 Broad Network Access 14
 - 1.3.3 Ressourcen-Pooling 14
 - 1.3.4 Rapid Elasticity 15
 - 1.3.5 Measured Services 15
 - 1.3.6 Pay-per-use 15
 - 1.4 Servicemodelle 15
 - 1.4.1 Infrastructure as a Service (IaaS) 15
 - 1.4.2 Platform as a Service (PaaS) 16
 - 1.4.3 Software as a Service (SaaS) 17
 - 1.5 Organisationsformen 18
 - 1.5.1 Public-Cloud 18
 - 1.5.2 Private-Cloud 19
 - 1.5.3 Hybrid-Cloud 20
 - 1.6 Cloud-Services 20
 - 1.6.1 Amazon 22
 - 1.6.2 Microsoft 22
 - 1.6.3 Salesforce.com 23
 - 1.6.4 DATEV eG 24

2 Risiken beim Cloud-Computing	27
2.1 Abhängigkeit vom Provider	27
2.2 Single Point of Failure	29
2.3 Datensicherheit	30
2.4 Datenschutz	31
2.5 Compliance	34
2.6 Vertrauen in die Cloud	36
3 Normen und Standards im Cloud-Computing	37
3.1 Grundlagen zu Normen und Standards	37
3.1.1 Definition	37
3.1.2 Ziele	38
3.1.3 Entwicklung und Nutzen im Unternehmen	39
3.1.4 Standard Setter	39
3.1.5 Relevante Standards für Cloud-Services	42
3.2 Übergreifende Management-Standards im Überblick	44
3.2.1 Allgemeine Risikomanagement-Standards	45
3.2.2 Standards für Wirtschaftsprüfer	50
3.2.3 Prüfungsstandards für Dienstleistungsunternehmen	52
3.2.4 Internationale ISA-Prüfungsstandards	56
3.3 Management-Standards mit Bezug zum Cloud-Computing	57
3.3.1 BSI-Sicherheitsempfehlungen für Cloud-Computing	58
3.3.2 EuroCloud	59
3.3.3 SaaS-EcoSystem und „Trust in Cloud“-Zertifizierung	61
3.3.4 GRC Stack der Cloud Security Alliance	62
3.3.5 NIST-User Cases for Cloud-Computing	64
3.3.6 IT Infrastructure Library (ITIL)	66
3.3.7 Control Objectives for Information and Related Technology (CobIT)	67
3.3.8 ISO/IEC 20000 Standard	69
3.3.9 ISO 27001 und IT Grundschutz (BSI-100 ff.)	70
3.3.10 German Cloud	73
3.3.11 COSO Enterprise Risk Management for Cloud-Computing	75
3.3.12 SOC 2	77
3.3.13 EU-Safe Harbor und EU-Standardvertragsklauseln	78
4 Der ISAE 3402-Standard	81
4.1 Einordnung in die Standardisierungs-Landkarte	82
4.2 Inhaltlicher Zweck und Anwendungsfall	87
4.3 Aufbau und Inhalte	92
4.3.1 Einleitung und „Scope“	93
4.3.2 Ziele des Audits	98

4.3.3	Definitionen	99
4.3.4	Übergreifende Anforderungen	105
4.3.5	Auditbezogene Anforderungen	114
5	Leitfaden für ein erfolgreiches ISAE 3402-Audit	125
5.1	Vorgehensweise im Überblick	126
5.2	Anforderungen der User Organisation	128
5.2.1	Entscheidung für die Cloud-Lösung	129
5.2.2	Einschätzung der Auswirkungen auf die Finanzberichterstattung	129
5.2.3	Auswahl eines adäquaten Auditierungsstandards	130
5.2.4	Finanz-Scoping: Identifizierung betroffener Cloud Services & Ressourcen	131
5.3	Vorbereitung	141
5.3.1	Rahmen und Leitlinien	141
5.3.2	Projektziele	144
5.3.3	Projektstruktur	145
5.3.4	Scope	152
5.3.5	Zeit- und Projektplanung	161
5.3.6	Auditor	162
5.3.7	Kommunikation	163
5.4	Implementierung und Dokumentation	164
5.4.1	Risikoidentifikation, -analyse und -evaluierung	165
5.4.2	Kontrolldesign	166
5.4.3	Systembeschreibung	167
5.4.4	Entity-Level-Controls	172
5.4.5	Activity-Level-Controls	182
5.4.6	3rd Party Controls	197
5.5	Audit	201
5.5.1	Readiness-Assessment	201
5.5.2	Behebung von Schwachstellen	203
5.5.3	ISAE 3402-Audit	204
5.5.4	Audit Report	206
5.6	Betrieb	206
5.6.1	Änderungsmanagement	207
5.6.2	Qualitätskontrollmaßnahmen	208
Anhang		211
Literatur		215

IT-Services in der Cloud und ISAE 3402

Ein praxisorientierter Leitfaden für eine erfolgreiche
Auditierung

Lissen, N.; Brünger, C.; Damhorst, S.

2014, XVII, 220 S. 80 Abb., Softcover

ISBN: 978-3-662-43472-7