

Nina Lissen
Christian Brünger
Stephan Damhorst

IT-Services in der Cloud und ISAE 3402

Ein praxisorientierter Leitfaden
für eine erfolgreiche Auditierung

 Springer Gabler

Nina Lissen
Christian Brünger
Stephan Damhorst

IT-Services in der Cloud und ISAE 3402

Ein praxisorientierter Leitfaden
für eine erfolgreiche Auditierung

IT-Services in der Cloud und ISAE 3402

Nina Lissen
Christian Brünger
Stephan Damhorst

IT-Services in der Cloud und ISAE 3402

Ein praxisorientierter Leitfaden für eine
erfolgreiche Auditierung

Nina Lissen
Düsseldorf
Deutschland

Stephan Damhorst
Düsseldorf
Deutschland

Christian Brünger
Universität Paderborn
Paderborn
Deutschland

ISBN 978-3-662-43472-7
DOI 10.1007/978-3-662-43473-4

ISBN 978-3-662-43473-4 (eBook)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Gabler

© Springer-Verlag Berlin Heidelberg 2014

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Lektorat: Michael Bursik

Assistenz: Janina Sobolewski

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Gabler ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-gabler.de

Vorwort

Die Nutzung von cloud-basierten IT-Services erfreut sich weltweit im privaten, kommerziellen und öffentlichen Bereich aufgrund ihrer erheblichen Ressourcen- und Effizienzvorteile zunehmender Beliebtheit und Anwendung.

Zum einen stellt diese Entwicklung einen bedeutenden Fortschritt und eine Realität dar, die aus unserer heutigen Welt und aus unserem Alltag nicht mehr wegzudenken ist.

Auf der anderen Seite werden seit einiger Zeit – nicht zuletzt mit beeinflusst durch die öffentliche Diskussion um Abhör- und Spionageskandale der weltweiten Geheimdienste – auch die Risiken der Datenspeicherung und Datenverarbeitung „in der Wolke“ an sich stärker in den Vordergrund gestellt. Ein steigendes Bedürfnis der Allgemeinheit nach Sicherheit und Transparenz im internationalen Datenverkehr ist die Folge.

Intention der Autoren ist es, mit dem Buch zu verdeutlichen, welche Risiken mit dem Cloud-Computing verbunden sind und wie sich diese reduzieren lassen. Dabei gehen die Autoren insbesondere auf den „klassischen“ Beispielfall der Auslagerung von rechnungslegungsrelevanten Cloud-Dienstleistungen einer Organisation an einen oder mehrere Cloud Service Provider ein.

Hierzu wird zunächst erläutert, welche Merkmale dem Cloud-Computing zuzuordnen sind und welche Herausforderungen sich daraus ergeben. Die gängigen Normen und Management-Standards im Cloud-Computing werden gegenüber gestellt und auf eine nachvollziehbare Weise erklärt. Es wird weiterhin beschrieben, für welche Anwendungsfälle der ISAE 3402 sich eignet, aus welchen Elementen er besteht – aber auch, wo die Grenzen seiner Anwendung liegen.

So wird auch aufgezeigt, wie in der Praxis damit umgegangen werden kann, dass der derzeit international gültige ISAE 3402-Standard derzeit die Unzulänglichkeit aufweist, sich nicht explizit auf alle cloud-relevanten Risiken zu beziehen. Diese ist aus Sicht der Autoren jedoch zu einem Großteil zu bewältigen mit einer Integration von Elementen des SOC 2-Standards, der selbst in Gänze derzeit nur in den USA gültig ist und derzeit kaum Erwähnung in Deutschland findet.

Ziel des Buches ist es letztlich, dem interessierten Leser und Anwender ein einfaches und robustes Vorgehensmodell zur Durchführung einer ISAE 3402–Auditing an die Hand zu geben, das nicht nur, aber auch gut von Cloud Service Providern und ihren

Kunden genutzt werden kann. Dieses wird untermauert durch die praxisorientierte Darstellung eines fiktiven Beispielvorgehens, das in vereinfachten, systematischen Schritten dargestellt wird.

Die herausgehobenen Schlüsselfaktoren für ein erfolgreiches Audit basieren dabei im Wesentlichen auf den praktischen Erfahrungen der Autoren.

Wir bedanken uns herzlich bei Herrn Dirk Skicki für sein Engagement hinsichtlich der fachlichen und systematischen Durchsicht des Buchentwurfs. Nicht zuletzt gilt unser Dank dem Springer Gabler Verlag und dem Lektor Michael Bursik für die freundliche Unterstützung und Geduld bei der Fertigstellung des Buches.

Düsseldorf und Paderborn im April 2014

Nina Lissen
Christian Brünger
Stephan Damhorst

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

Über die Autoren



Dr. Christian Brünger studierte Betriebswirtschaft in Bielefeld und Paderborn mit den Schwerpunkten Risikomanagement und Finanzwirtschaft. Er leitet operativ das Forschungszentrum für Risikomanagement an der Universität Paderborn. Er ist Autor zahlreicher Fachpublikationen im Bereich Risikomanagement und Lehrbeauftragter an Universitäten und Fachhochschulen. Zudem ist er auch Bereichsleiter eines mittelständischen Systemhauses und Cloud Service Providers und dort verantwortlich für internationale IT-Projekte.



Stephan Damhorst Jahrgang 1972, ist studierter Betriebswirt und beschäftigt sich seit dem Jahre 2000 in Theorie und Praxis mit der Implementierung von Managementsystemen sowie der IT Compliance in Unternehmen.

Neben seiner Tätigkeit als Fachexperte für IT Service Management und Informationssicherheit bei einem globalen Bildungsdienstleister in Bayern ist der zertifizierte ITIL Expert seit 2006 bei dem internen IT Service Provider eines international aufgestellten Industriekonzerns im Ruhrgebiet tätig. Zu seinem Verantwortungsgebiet zählen neben der Steuerung des IT Risikoportfolios ebenfalls die Auditierung rechnungslegungsrelevanter Systeme im Konzern auf Basis des ISAE 3402 Standards.



Nina Lissen Jahrgang 1973, ist Diplom-Ökonomin und studierte Wirtschaftswissenschaften mit den Schwerpunkten Controlling und Wirtschaftspolitik in Duisburg. Parallel zum Studium absolvierte sie Ausbildungen zur Industriekauffrau und Fremdsprachenkorrespondentin bei der Mannesmann-Röhrenwerke AG. Seit 2005 ist sie im Bereich Finance bei der E-Plus Gruppe in Düsseldorf beschäftigt, baute das Risikomanagement dort mit auf und war viele Jahre lang für das Interne Kontrollsystem der E-Plus Gruppe verantwortlich; in dieser Funktion leitete sie zahlreiche Assurance-, SAS70- und ISAE 3402 -Audits an diversen Standorten. Von 2010 bis 2012 war sie Vorstandsmitglied der Risk Management Association e. V. in München, des Expertennetzwerks der Risikomanager im deutschsprachigen Raum. Seit 2013 ist sie Senior Managerin im Bereich Financial Control der E-Plus Gruppe und beschäftigt sich mit der Erstellung und Optimierung der laufenden Finanzberichterstattung an die Geschäftsführung und an KPN Mobile International.

Abkürzungsverzeichnis

AO	Abgabenordnung
ASP	Application-Service-Providing
BDSG	Bundesdatenschutzgesetz
BilMoG	Bilanzrechtsmodernisierungsgesetz
BMELV	Bundesverbraucherministerium
BMWi	Bundesministerium für Wirtschaft und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSP	Cloud Service Provider
d. h.	das heißt
ECP	Europäische Cloud Partnerschaft
ENISA	Europäische Agentur für Netz- und Informationssicherheit
ERP	Enterprise Resource Planning
etc.	et cetera
ETSI	Telecommunications Standards Institute
EU	Europäische Union
EWR	Europäischen Wirtschaftsraums
GDBdU	Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	Grundsätzen ordnungsgemäßer Buchführung
GoBS	Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
IaaS	Infrastructure as a Service
ITIL	IT Infrastructure Library
PaaS	Platform as a Service
RFR	reliable financial reporting
SaaS	Software as a Service
SGB	Sozialgesetzbuch
SLA	Service Level Agreement
SOA	service-orientierte Architekturen
VPN	virtuelle private Netzwerke

Abbildungsverzeichnis

Abb. 1.1	Überwachung durch den US-Geheimdienst NSA	6
Abb. 1.2	Meilensteine in der Informationstechnologie	8
Abb. 1.3	Basistechnologien und Konzepte	10
Abb. 1.4	Cloud-Computing Merkmale	14
Abb. 1.5	Service Modelle	16
Abb. 1.6	Organisationsformen	18
Abb. 1.7	Amazon Web Services	22
Abb. 1.8	Microsoft Windows Azure	23
Abb. 1.9	Salesforce.com	24
Abb. 1.10	DATEV Cloud	25
Abb. 2.1	Risiken im Cloud-Computing	28
Abb. 2.2	Bundesdatenschutzgesetz	32
Abb. 2.3	Auftragsdatenverarbeitung	33
Abb. 3.1	Zusammenarbeit der Standardisierungsorganisationen	42
Abb. 3.2	Standardisierungsorganisationen und Konsortien	43
Abb. 3.3	COSO-ERM-Würfel	47
Abb. 3.4	Siebzehn Prinzipien des COSO 2013	49
Abb. 3.5	Überblick über die Prüfungsanforderungen für Dienstleistungsunternehmen	54
Abb. 3.6	EuroCloud Logo	61
Abb. 3.7	Beispielhaftes Zertifikat für „Trust in Cloud“	63
Abb. 3.8	GRC Stack Logo	64
Abb. 3.9	ITIL Framework	66
Abb. 3.10	ITIL Logo	67
Abb. 3.11	Die 5 COBIT-Prinzipien	68
Abb. 3.12	Die COBIT Enabler	69
Abb. 3.13	Beispiel eines ISO 27001-Zertifikates	72
Abb. 3.14	German Cloud Logo	74
Abb. 3.15	Verlust der Management-Aufsicht im Cloud Umfeld	75
Abb. 3.16	ERM Prozess für Cloud Lösungen im COSO ERM Modell	76

Abb. 3.17	Cloud spezifischer COSO ERM-Würfel	76
Abb. 4.1	Neun übergeordnete Herausforderungen für Cloud-Computing	83
Abb. 4.2	Herausforderungen im Cloud Computing	84
Abb. 4.3	Standardisierungslandkarte für Cloud-Computing	85
Abb. 4.4	Beziehung zwischen Wirtschaftsprüfer, Service- und Userorganisation	89
Abb. 4.5	Einordnung des Wirtschaftsprüfungsauftrages	94
Abb. 4.6	Three lines of defense model	101
Abb. 4.7	ISAE 3402 Beziehungen	103
Abb. 4.8	Komponenten des internen Kontrollsystems	115
Abb. 4.9	Beziehung der Prozessschritte	116
Abb. 4.10	Struktur von Prüfberichten nach ISAE 3402	123
Abb. 5.1	Service-Strukturen	126
Abb. 5.2	Vorgehensweise <i>ISAE 3402-Audit</i> im Überblick	127
Abb. 5.3	Aufgliederung der GuV-Positionen	137
Abb. 5.4	Scoping in der User-Organisation	142
Abb. 5.5	Zielpyramide eines IKS-Projektes	144
Abb. 5.6	Beispiel eines Masterplans eines ISAE 3402-Projektes	145
Abb. 5.7	Exemplarische Projektorganisation	146
Abb. 5.8	Exemplarische Dokumentation der Tester-Objektivität	150
Abb. 5.9	Vorgehen zum ISAE-Scoping	153
Abb. 5.10	Exemplarische Dokumentation des Scopings für Cloud-Services	155
Abb. 5.11	Exemplarische Dokumentation der IT-Ressourcen für Cloud-Services	157
Abb. 5.12	COBIT 5 Prozessreferenzmodell	159
Abb. 5.13	Priorisierung der COBIT-Prozesse (COBIT 4.1)	160
Abb. 5.14	COBIT und PCAOB	161
Abb. 5.15	Exemplarischer Zeitplan eines ISAE 3402-Projektes	162
Abb. 5.16	Exemplarische Dokumentation der Eskalationsprozesse	173
Abb. 5.17	COBIT 5 Prozessreferenzmodell „Evaluieren, Vorgeben und Überwachen“	174
Abb. 5.18	Exemplarische Dokumentation einer Entity-Level Kontrolle	175
Abb. 5.19	COBIT 5 Prozessreferenzmodell für das IT-Management	183
Abb. 5.20	Übersicht möglicher Activity-Level-Kontrollen	184
Abb. 5.21	Ebenenkonzept in der Prozessanalyse	194
Abb. 5.22	Darstellungsbeispiel – Einbettung Kontrolle in Geschäftsprozess	196
Abb. 5.23	Exemplarische Dokumentation einer Activity-Level-Kontrolle	197
Abb. 5.24	Sub-Service-Strukturen	198
Abb. 5.25	Exemplarische Dokumentation der Sub-Services für Cloud-Services	199