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

Springer Gabler

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

Springer Gabler

Nina Lissen
Düsseldorf
Deutschland

Christian Brünger
Universität Paderborn
Paderborn
Deutschland

Stephan Damhorst
Düsseldorf
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

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–Auditierung 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

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	Bilanzrechtsmoderisierungsgesetz
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 Libary
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