

Cloud-Computing birgt für Unternehmen, für die öffentliche Verwaltung und private Haushalte nicht nur erhebliche Potenziale, sondern ist ebenfalls mit bedeutenden Herausforderungen und Risiken verbunden.

► **Definition** „Ein Risiko kennzeichnet eine Eventualität, dass mit einer (ggf. niedrigen, ggf. auch unbekannten) Wahrscheinlichkeit ein (ggf. hoher, ggf. in seinem Ausmaß unbekannter) Schaden bei einer (wirtschaftlichen) Entscheidung eintreten oder ein erwarteter Vorteil ausbleiben kann.“ (Vgl. Springer Gabler 2014d).

Neben der Abhängigkeit vom Cloud Service Provider und einem damit mitunter verbundenen Verlust an Kontrolle und Transparenz sind eine unzureichende Datensicherheit, der mögliche Verstoß gegen gesetzliche Vorgaben sowie unzureichende Verfügbarkeit und Performance der Cloud-Services die am häufigsten genannten Risiken, die im Zusammenhang mit Cloud-Computing genannt werden. Im nachfolgenden Kapitel werden die für Cloud-Computing typischen Risiken in Anlehnung an den 2012 erschienenen COSO ERM Leitfaden für Cloud-Computing dargestellt und aufgezeigt, wie die Herausforderungen angegangen werden können (Abb. 2.1) (Vgl. Horwath et al. 2012; vgl. Kap. 3.3.11).

2.1 Abhängigkeit vom Provider

Zwischen Cloud Service Provider (CSP) und Kunde wird in der Regel ein Cloud-Computing-Vertrag geschlossen. Dieser enthält unter anderem die detaillierte Leistungsbeschreibung des Cloud-Service sowie die entsprechenden Konditionen der Serviceerbringung (Laufzeit und Vergütung).

Zusätzlich bieten viele CSPs ihren Kunden Tools zur Entwicklung eigener Cloud-Services an. Sind diese Entwicklungs-Tools proprietär, funktionieren sie oftmals nur in der vom CSP bereitgestellten Architektur.

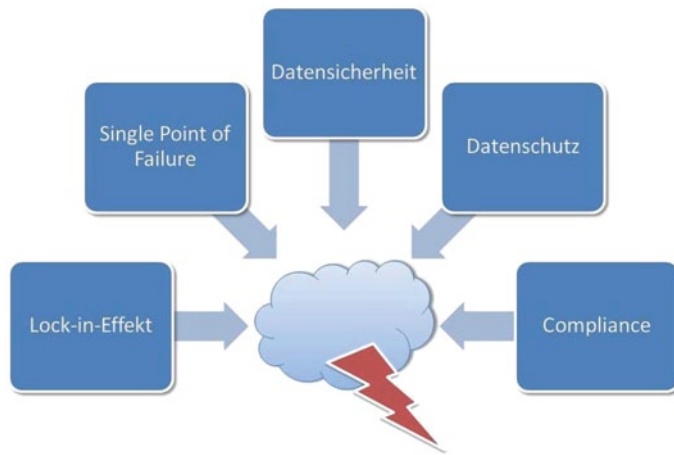


Abb. 2.1 Risiken im Cloud-Computing. (Quelle: Eigene Abbildung)

Sowohl durch die Vertragslaufzeit als auch durch die technologischen Einschränkungen entsteht für den Kunden in der Regel ein Abhängigkeitsverhältnis zum CSP.

Der Wechsel zu einem anderen CSP oder die Rückabwicklung zum Eigenbetrieb sind dem Kunden nicht immer sofort oder nur mit höherem Kostenaufwand möglich.

In der Betriebswirtschaft werden Kosten, die eine Änderung der aktuellen Situation aufgrund hoher Wechselkosten unwirtschaftlich machen, als Lock-in-Effekt (von engl. to lock in: einschließen, einsperren) bezeichnet.

Gerät beispielsweise der CSP oder einer der Subunternehmer in die Insolvenz, ist es für den Kunden nicht direkt nachvollziehbar, was mit dem Rechenzentren, Servern und Datenbanken geschieht, auf denen seine Daten gespeichert sind.

Zusätzlich wird das Risiko des unberechtigten Zugriffs auf Daten erhöht.

Tipp aus der Praxis

Um die Abhängigkeit vom CSP zu begrenzen, ist es ratsam, eine **Ausstiegs-Strategie** für den konkreten Cloud-Service zu erstellen. In dieser sollte der Wechsel zu einem anderen CSP oder die Überführung in den Eigenbetrieb konkret vorhergesehen und beschrieben werden.

Kommt es bei einer Rückabwicklung zu einer gerichtlichen Auseinandersetzung, ist der **vereinbarte Gerichtsstand** hinsichtlich der Urteilsvollstreckbarkeit von besonderer Bedeutung.

Eine im Cloud-Computing-Vertrag festgelegte **Schiedsklausel** stellt in vielen Fällen eine geeignete Alternative zum Verfahren vor staatlichen Gerichten dar. Auch sollte der erforderliche Service Level (Verfügbarkeit, Performance sowie Reaktions- und Wiederherstellungszeiten) in einem Service Level Agreement (SLA) mit dem CSP vereinbart werden.

Nach Einschätzung der Autoren lassen sich die beschriebenen Risiken aus Kundensicht jedoch nicht völlig vermeiden.

2.2 Single Point of Failure

Ist ein CSP durch technische oder organisatorische Einflüsse zeitweise nicht mehr in der Lage, den Cloud-Service zu erbringen, kann dies ein erhebliches geschäftliches Risiko für den Benutzer haben (Vgl. Eriksdotter 2011).

Eine zeitweise nicht verfügbare online-Plattform stellt für den genannten Online-Automaat beispielsweise ein solches geschäftliches Risiko dar. Der Ausfall würde einen erheblichen Imageschaden für das Unternehmen bedeuten sowie aufgrund abgebrochener oder erst gar nicht durchgeführter Transaktionen zu erheblichen Umsatzeinbußen führen.

Neben der Verfügbarkeit besteht ein weiteres Risiko in der unzureichenden Performance. Ist ein Cloud Service Provider beispielsweise aufgrund eines fehlenden Change Managements nicht in der Lage den Cloud-Service bei erhöhter Nutzung entsprechend zu skalieren, so kann es zu kurzfristigen Kapazitätsproblemen kommen, unter denen die Performance des Systems zu leiden hat.

Um diese Risiken zu beherrschen, verwenden Cloud Service Provider in der Regel Hochverfügbarkeits-Architekturen.

Der Benutzer ist jedoch selbst nicht mehr in der Lage, die technischen Anpassungen an den Cloud-Service vorzunehmen. Er ist vielmehr darauf angewiesen, dass erforderlichen Änderungen vom CSP geplant, sicher und ohne Auswirkungen auf die Verfügbarkeit oder Performance des Cloud-Service durchgeführt werden.

Tipp aus der Praxis

Auch beim Risiko „Single Point of Failure“ ist es grundsätzlich sinnvoll, mit dem CSP Vereinbarungen hinsichtlich der **Reaktions- und Wiederherstellungszeiten** im Fehlerfall zu treffen. Die Implementierung eigener Systeme zur Überwachung der Verfügbarkeit der Cloud-Services kann ebenfalls hilfreich sein.

Ein standardisiertes Change-Request-Verfahren sowie ein entsprechendes **Notfall-Management**¹ sollte im Cloud-Computing-Vertrag vereinbart und jährlich zum Beispiel im Rahmen eines ISAE 3402 Audits auf Wirksamkeit überprüft werden.

Diese Maßnahmen ersetzen letztlich jedoch nicht einen umfangreichen Notfall-Plan, welcher bei einem längeren Systemausfall zu tragen kommt. Der Notfall-Plan

¹ Zu diesem Themenkomplex sind in der gängigen Literatur auch unter der Bezeichnung „Business Continuity Management“ wertvolle Hinweise und weiterführende Standards (z. B. ISO 22301) zu finden.

sieht beispielsweise vor, wie Kopien des Cloud-Service bei einem anderen CSP in Betrieb genommen werden können.

Nach Einschätzung der Autoren lassen sich die beschriebenen Risiken aus Kundensicht jedoch nicht völlig vermeiden.

2.3 Datensicherheit

Durch die Auslagerung in die Cloud verlieren die Kunden den direkten Einfluss auf die *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* der eigenen Daten. Insofern ist es wenig überraschend, dass Bedenken hinsichtlich der Datensicherheit in der Cloud in Umfragen an erster Stelle genannt werden.

► **Definition** Unter **Vertraulichkeit** wird in diesem Zusammenhang verstanden, dass Daten in der Cloud vor unbefugtem Zugriff geschützt sind.

Verfügbarkeit bezeichnet den Umstand, dass dem Benutzer die in der Leistungsbeschreibung benannten Eigenschaften zum vereinbarten Zeitpunkt zur Verfügung stehen.

Die **Integrität** von Daten ist dann gegeben, wenn diese vollständig und unverändert sind.

Die Bedenken sind durchaus berechtigt, da CSPs ein attraktives Ziel für Hacker und Cyberangriffe darstellen. Unter einem Cyberangriff versteht man einen elektronischen Angriff, der über eine Netzwerkverbindung erfolgt. Der Angriff findet im virtuellen Cyber-Raum statt und richtet sich beispielsweise gegen einzelne Cloud-Services oder einen CSP. Der Angreifer hat zum Ziel, die Sicherheitsbarrieren der Systeme zu durchbrechen, um beispielsweise sensible oder geheime Daten auszuspähen.

Ein anderes Beispiel zeigt auf, dass der Schutz sensibler Daten mit den üblichen Mitteln nicht immer gewährleistet ist. Oftmals müssen Daten gelöscht werden, zum Beispiel nach einem beendeten Auftrag. Hier entsteht das Risiko, das Daten auf den Plattformen und Datenbanken nicht vollständig oder unzureichend gelöscht werden. Dritte können mitunter auf Daten zugreifen, wenn die Trennung der Mandanten unzureichend gesichert ist. In der Cloud werden unterschiedliche Mandanten nicht zwingend physikalisch getrennt.

Tipp aus der Praxis

Bereits in der Planungsphase sollte eine **Sicherheitsanalyse** durchgeführt werden, um Varianten für die Auslagerung zu konzipieren, den Schutzbedarf der Daten zu bestimmen sowie eine Risikoanalyse durchzuführen. Diese Informationen werden verwendet, um konkrete **Sicherheitsanforderungen** zu definieren, die zu jeder Zeit erfüllt sein müssen.

Mit Beginn der Transition-Phase sollte eine eindeutige **Leistungsbeschreibung** zur Gewährleistung der Qualität und Datensicherheit erstellt werden. Die technische Migration der Systeme erfolgt dann schrittweise nach den Vorgaben der beschriebenen Sicherheitsanforderungen.

Über organisatorische Maßnahmen sollte der CSP in der Betriebsphase sicherstellen, dass die Sicherheit der Rechenzentren, der Daten, der Plattformen sowie der Cloud-Services gewährleistet ist. Zu diesen Maßnahmen gehört die Umsetzung konkreter Sicherheitsmaßnahmen entsprechend der Vorgaben des **IT-Grundschutz-Kataloges** des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

2.4 Datenschutz

Mit der Benutzung von Cloud-Services werden vielfältigste Daten und Informationen gespeichert und verarbeitet, deren Schutzwürdigkeit von „unbedeutend“ bis „besonders hoch“ reichen kann.

Das Ziel von Datenschutz ist es dabei, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.²

► **Definition „personenbezogene Daten“** „Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse) einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).“ Personenbezogene Daten sind zum Beispiel Name, Anschrift, Geburtsdatum, usw.

Beim Cloud-Computing werden personenbezogene Daten mitunter in den weltweit verteilten Rechenzentren des Cloud Service Providers verarbeitet, ohne dass der Benutzer des Cloud-Services mitunter Kenntnis darüber hat „wie“, „wo“ und „durch wen“ die Verarbeitung erfolgt. Hier gilt es, insbesondere das territoriale Schutzniveau zu beachten, das in den Staaten gilt, in denen die Daten in den Cloud-Service eingebracht werden (Abb. 2.2).

Unter dem territorialen Schutzniveau werden nationale Bestimmungen verstanden, nach denen besonders schützenswerte Daten in bestimmte Territorien (zum Beispiel EU-Raum, in die USA oder in Drittstaaten) nicht oder nur unter besonderen Voraussetzungen verbracht werden dürfen.

Welches nationale Recht im Einzelfall zur Anwendung kommt, ist in Artikel 4 der Datenschutzrichtlinie 95/46/EG in Verbindung mit § 1 Absatz 5 Bundesdatenschutzgesetz geregelt. Im Zusammenhang mit Cloud-Services können demnach zwei Anwendungsfälle unterschieden werden.

² Vgl. § 1 Abs. 1 BDSG.

Bundesdatenschutzgesetz (§ 11)

Übermittlung **personenbezogener Daten** an Staaten
außerhalb der EU ist grundsätzlich untersagt!



- Cloud-Nutzer ist verantwortlich und haftet
- Cloud-Nutzer muss sich davon überzeugen, dass der Cloud-Anbieter hinsichtlich der technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet

Abb. 2.2 Bundesdatenschutzgesetz. (Quelle: Eigene Abbildung)

Hat der Benutzer des Cloud-Services seinen Sitz innerhalb der EU oder den Ländern des Europäischen Wirtschaftsraums (EWR), so ist das Recht des Landes des Benutzers des Cloud-Services anzuwenden. Der Benutzer des Cloud-Services wird als „verantwortliche Stelle“ qualifiziert und hat somit die gesetzlichen Verpflichtungen im Rahmen der Auftragsdatenverarbeitung zu erfüllen.

Hat der Benutzer des Cloud-Services seinen Sitz außerhalb der EU oder den Ländern des Europäischen Wirtschaftsraums (EWR), aber beauftragt einen Cloud Service Provider, der innerhalb des EWR niedergelassen ist, so ist das Recht des Staates anzuwenden, in dem der Cloud Service Provider seine Niederlassung hat. Der Cloud Service Provider wird in diesem Fall als datenschutzrechtlicher Auftragnehmer qualifiziert (Abb. 2.3).

Eine Besonderheit des deutschen Rechts besteht darin, dass die Anwendung der Auftragsdatenverarbeitung nur dann erlaubt ist, wenn der Cloud Service Provider seinen Sitz innerhalb der EU oder den Ländern des Europäischen Wirtschaftsraums (EWR) hat und die Daten auch dort verarbeitet werden.³

Eine Übermittlung von personenbezogenen Daten in Drittländer (Länder außerhalb der EU/EWR) wird nur dann gestattet, wenn ein angemessenes Datenschutzniveau sichergestellt werden kann.⁴ Die rechtskonforme Übermittlung kann auf folgenden Grundlagen erfolgen:

- Angemessenheitsentscheidung der Europäischen Kommission (Schweiz, Kanada und Argentinien),
- Unterzeichnung von EU-Standardvertragsklauseln,
- Ausnahmen gemäß Artikel 26 Richtlinie 95/46/EG,
- Safe Harbour.

³ Vgl. § 3 Abs. 8 BDSG.

⁴ Vgl. § 4b Abs. 2, 3 BDSG und Art. 25, 26 Richtlinie 95/46/EG.

Abb. 2.3 Auftragsdatenverarbeitung. (Quelle: Eigene Abbildung)



Die Verwendung der „Safe Harbor Principles“, einer Datenschutzvereinbarung zwischen der Europäischen Union und den United States of America (USA) für Verträge mit Cloud Service Providern aus den USA, ist unter den Fachexperten jedoch stark umstritten.

Eine einfache Selbst-Zertifizierung des Cloud Service Providers nach „Safe Harbor“ reicht nach Ansicht der European Privacy Seal (EuroPriSe) für sich genommen nicht aus, da insoweit keine tatsächliche Durchsetzung der Datenschutz-Anforderungen insbesondere im Cloud-Computing erfolgt.⁵

Die Arbeitsgruppe fordert daher von Benutzern von Cloud-Services, sich nicht allein auf die Selbst-Zertifizierung zu verlassen, sondern die Einhaltung der Prinzipien nachweislich zu überprüfen.

Wie aus den Ausführungen deutlich wird, ergibt sich bei der Betrachtung der rechtlichen Risiken von Cloud-Computing eine gewisse Komplexität. Zudem sollte neben der aktuellen Rechtslage auch die zukünftige Entwicklung des Datenschutzes sowie der politischen Rahmenbedingungen betrachtet werden.

⁵ <http://www.europaen-privacy-seal.eu>.

Tipp aus der Praxis

Die Verwendung eines Cloud-Services, zum Beispiel eines cloud-basierten CRM Systems, erfordert in der heutigen Zeit lediglich einen Internet-Zugang sowie eine Kreditkarte. So kann es für die Marketing-Abteilung sehr verlockend sein, diesen Cloud-Service für die anstehende Marketing-Kampagne einzusetzen – und das ganz ohne die IT Abteilung miteinzubeziehen. Es ist leicht vorstellbar, dass in diesem System neben personenbezogenen Kundendaten ebenfalls sensible Unternehmensinformationen abgespeichert werden.

Es wird daher empfohlen, den unkontrollierten Einsatzes von Cloud-Services mittels einer unternehmensweit gültigen **Cloud-Policy** zu regeln.

Die Cloud-Policy sollte darüber Auskunft geben, welche **Geschäftsprozesse** und welche **Daten** für cloud-basierte Services in der Organisation zugelassen sind. Darüber hinaus sollte aus der Policy hervorgehen, auf welchem Wege Cloud-Services beschafft werden können und welche CSP von der Organisation präferiert werden.

2.5 Compliance

Compliance (auch Regelkonformität) steht für die Einhaltung von Vorschriften und Richtlinien in Organisationen, aber auch von freiwilligen Kodizes.

Hinweis

Im Zusammenhang mit dem Cloud-Computing ist hier zu beachten, dass der Nutzer von Cloud-Services vor dem Gesetz **für die Sicherheit seiner Daten und die Einhaltung von Compliance-Anforderungen verantwortlich ist und die Einhaltung der ihn betreffenden rechtlichen Bestimmungen gewährleisten muss**; auch wenn die Daten auf einem Rechner in der Cloud gespeichert und verarbeitet werden.

Die Compliance Anforderungen an den CSP sowie den Nutzer von Cloud-Services können dabei entsprechend der Organisation sehr unterschiedlich sein. Sie ergeben sich in der Regel aus Kriterien wie zum Beispiel der Branche, der Rechtsform, dem Hauptsitz der Organisation, dem Ort der Leistungserbringung oder durch den Cloud-Service.

Werden beispielsweise rechnungslegungsrelevante Services in der Cloud betrieben, so gilt es im Rahmen des Jahresabschlusses eine Vielzahl spezifischer Anforderungen zu berücksichtigen.

Anforderungen ergeben sich unter anderen aus:

- dem Handelsgesetzbuch (HGB),
- dem Sozialgesetzbuch (SGB),
- der Abgabenordnung (AO),
- den Grundsätzen ordnungsgemäßer Buchführung (GoB),
- den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS),
- den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU),
- den Prüfungsstandards der Wirtschaftsprüfer (z. B. IDW PS 330),
- dem Bundesdatenschutzgesetz (BDSG) sowie
- dem Bilanzrechtsmodernisierungsgesetz (BilMoG).

Cloud Service Provider sowie die Benutzer von Cloud-Services sind gut beraten, die konkreten Compliance-Anforderungen in jedem Falle individuell zu ermitteln.

Der Benutzer von Cloud-Services hat dabei weitreichende Einfluss- und Kontrollmöglichkeiten, um die zur Einhaltung rechtlicher Bestimmungen notwendige Transparenz sicherzustellen.

Wie bereits an anderer Stelle erwähnt, kommt dem Service Level Agreement (SLA) zur Absicherung der Vertraulichkeit, Verfügbarkeit und Integrität der Daten eine besondere Bedeutung zu:

Im SLA sollte unter anderem festgeschrieben werden, wie der CSP die Sicherheit der Daten gewährleistet, auf welche Weisen die entsprechenden Maßnahmen überprüft werden können, wo die Daten gespeichert werden sowie wie und wer auf die Daten Zugriff hat.

Um die Einhaltung der Compliance-Anforderungen sicherzustellen, sollte das interne Kontrollsystem die speziellen Problemstellungen beim Einsatz von Cloud-Computing berücksichtigen.

Das interne Kontrollsystem eines Cloud Service Providers kann dabei auch Gegenstand der Abschlussprüfung bei deren Kunden sein.

Der Abschlussprüfer hat dabei die Aufgabe, die Wirksamkeit des internen Kontrollsystems zu festzustellen und überprüft dabei, ob bei der Nutzung von Cloud-Services rechnungslegungsrelevante Anforderungen erfüllt werden.

Die Nichterfüllung von Compliance-Anforderungen kann für das Unternehmen weitreichende Folgen haben. Neben Vertragsstrafen und Bußgeldern können möglicherweise Schadensersatzansprüche gegen das Unternehmen geltend gemacht werden.

Im Zusammenhang mit öffentlichen Auftraggebern kann es bis zum Ausschluss von Ausschreibungsverfahren führen.

Letztendlich erleidet das Unternehmen durch die Nichteinhaltung von Compliance-Anforderungen einen erheblichen Imageschaden und muss in der Folge nicht selten den Verlust von Marktanteilen tragen.

Tipp aus der Praxis

Durch die Nutzung von Cloud-Services wird mit dem Cloud Service Provider zwar ein Dritter zur Erbringung der Dienstleistung eingesetzt, in der Regel bleibt aber der Benutzer für die Erfüllung der individuellen Compliance-Anforderungen verantwortlich und hat etwaige Konsequenzen bei Nichterfüllung zu tragen.

Um dieser Verantwortung gerecht zu werden, wird die Definition einer unternehmensweit gültigen Guideline zur Klassifizierung von Daten empfohlen. Die Guideline sollte unterschiedliche Schutzklassen für Daten definieren und sicherheitsrelevante Anforderungen festlegen, die von der Organisation zu befolgen sind.

Letztlich gilt es, alle relevanten Daten im Unternehmen nach Maßgabe der Guideline einzuordnen und die Zugriffsrechte auf diese Informationen entsprechend der Guideline zu überprüfen.

Im Zweifelsfall sollten sich Unternehmen sich hinsichtlich der individuell auf ihr Unternehmen zutreffenden relevanten Compliance-Anforderungen beraten lassen.

2.6 Vertrauen in die Cloud

Mit der Entscheidung zur Auslagerung von IT-Services in die Cloud ist für den Kunden (User Organisation) oftmals der Verlust an Transparenz verbunden. Durch den Verlust des direkten Einblicks in die eigenen Geschäfts- und IT-Prozesse und Ressourcen können Sorgen und Unsicherheiten entstehen. An dieser Stelle werden u. a. häufig Themen wie mangelnder Einblick in Fragen des Datenschutzes und in die Datensicherheit beim CSP genannt.

Insbesondere kann der Kunde aber auch die „Hoheit“ über Prozesse zur Erstellung seiner externen Rechnungslegung verlieren. Diese Themen sind nicht zu vernachlässigen, da die Haftung für die korrekte Abwicklung zu diesen Themen trotz Auslagerung bei der User Organisation verbleibt und diese die Verantwortung hat nachzuweisen dass Prozesse ordnungsgemäß und korrekt in seinem Sinne abgewickelt wurden.

Daher wiederum spielen diese Themen nicht zuletzt für Cloud-Service Kunden – und damit auch für den CSP selbst – eine übergeordnete Rolle bei der Entscheidung für die Nutzung eines Cloud-Services bzw. bei der Vertragsgestaltung zu einem Cloud-Service.

Durch die Vereinbarung eines sachgerechten internen Kontrollsystems und der Erfüllung des *ISAE 3402-Audit* kann der Cloud Service Provider wie in diesem Buch beschrieben gegenüber seinen Kunden Transparenz darüber schaffen, wie Anforderungen an Datenschutz, Datensicherheit und Compliance gemäß der aktuellen Anforderungen gewährleistet werden.

Somit entsteht ein Fundament für das notwendige Vertrauen in die Cloud.

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