Eine Veröffentlichung des ISACA Germany Chapter e.V.
Fachgruppe Cloud Computing in Kooperation mit dem BSI

Leitfaden
Anwendung des BSI C5 durch Interne Revision und Informationssicherheit

ISACA
Trust in, and value from, information systems
Germany Chapter

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e.V.
Oberwallstrasse 24
10117 Berlin

www.isaca.de
info@isaca.de

Autorenteam:
- Dr. Clemens Doubrava (BSI)
- Lars Hawranek (Bausparkasse Schwäbisch Hall AG)
- Michael Herrmann (SAP SE)
- Ralf Herter (BASF Business Services GmbH)
- Markus J. Neuhaus (marim consult)
- Michael Neuy (ARD ZDF Deutschlandradio Beitragsservice)
- Alexander W. Koehler (ICT Economic Impact)
- Peter Reiner (Fujitsu Technology Solutions GmbH)
- Edgar Röder
- Katharina Schmied (Diebold Nixdorf)
- Eberhard Scheuble (Akamai Technologies)
- Folker Scholz (FSU)
- Dr. Karl-Friedrich Thier (T-Systems International GmbH)

Die Inhalte dieses Leitfadens wurden von Mitgliedern des ISACA Germany Chapter e.V. in Kooperation mit dem BSI erarbeitet und sind sorgfältig recherchiert. Trotz größtmöglicher Sorgfalt erhebt die vorliegende Publikation keinen Anspruch auf Vollständigkeit. Sie spiegelt die Auffassung des ISACA Germany Chapter wider. ISACA Germany Chapter e.V. übernimmt keine Haftung für den Inhalt.

Der jeweils aktuelle Leitfaden kann unter www.isaca.de/c5 kostenlos bezogen werden. Alle Rechte, auch das der auszugsweisen Vervielfältigung, liegen beim ISACA Germany Chapter e.V.

Stand: September 2017 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe Cloud Computing)

Leitfaden

Anwendung des BSI C5 durch Interne Revision und Informationssicherheit

ISACA®
Trust in, and value from, information systems
Germany Chapter

Vorwort

ISACA Germany Chapter e.V.

Immer mehr Unternehmen setzen in der digitalen Transformation auf Cloud Computing. Cloud-Dienste treffen zunehmend die Anforderungen des Business, während On-Premise-Lösungen zurückgedrängt werden. Viele Unternehmen tun sich bei der Auswahl von Cloud-Anbietern jedoch immer noch schwer, die Risiken im Hinblick auf Informationssicherheit und Compliance angemessen zu bewerten. Häufig fehlt es dabei an objektiven Prüfkriterien und Mindestanforderungen, die sämtliche relevanten Aspekte der Cloud-Nutzung abdecken. Diesem Bedürfnis hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Veröffentlichung des Anforderungskatalogs Cloud Computing (C5) zur Beurteilung der Informationssicherheit von Cloud-Diensten Rechnung getragen, von dem sowohl die Kunden als auch die Anbieter von Cloud-Dienstleistungen profitieren.

Als Verband von IT-Revisoren, Informationssicherheitsmanagern und IT-Governance-Experten wissen wir aus Befragungen unserer Mitglieder, dass es diesen Berufsgruppen noch an Orientierung vor allem bei der Prüfbarkeit von Cloud-Dienstleistungen fehlt. Um diese Lücke praxisnah zu füllen, haben die Fachgruppe Cloud Computing des ISACA Germany Chapter und das BSI gemeinsam den vorliegenden Leitfaden zur Anwendung des Anforderungskatalogs C5 durch Interne Revision und Informationssicherheit entwickelt. Mit dieser Publikation setzen wir unsere erfolgreiche Kooperation mit dem BSI fort, die 2013 mit der Entstehung des Leitfadens »Cyber-Sicherheits-Check« ihren Anfang genommen hat.

Wir bedanken uns herzlich bei den Autoren dieses Leitfadens und wünschen Ihnen eine informationsreiche Lektüre.

Dr. Tim Sattler
Vorstand ISACA Germany Chapter e.V
Ressort Facharbeit und Arbeitskreise

Dr. Matthias Goeken
Vorstand ISACA Germany Chapter e.V.
Ressort Publikationen

Bundesamt für Sicherheit in der Informationstechnik

Als nationale Cyber-Sicherheitsbehörde gestaltet das BSI die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft. Cloud Computing ist ein wichtiger Bereich in der Digitalisierung und hierfür hat das BSI mit dem Cloud Computing Compliance Controls Catalogue – kurz C5 – die Mindestanforderungen an Cloud-Computing-Anbieter definiert. Es verbleibt die Herausforderung, wie ein potenzieller Cloud-Nutzer das Vertrauen entwickeln kann, dass ein Cloud-Anbieter für ihn genügend Sicherheit bietet.

Anders als bei den Sicherheitsanforderungen ist der letzte Punkt allein vom Kunden und seinem Risikoappetit abhängig. Hier sind viele Wege denkbar. Als BSI haben wir im C5 einen Weg dazu aufgezeigt, nämlich die Einhaltung der C5-Anforderungen über ein Testat eines Wirtschaftsprüfers zu belegen und die Anforderungen sowie die regelmäßige Vorlage des Berichts vertraglich zwischen Cloud-Anbieter und Cloud-Kunde zu vereinbaren. In diesem Papier adressiert das BSI gemeinsam mit der ISACA die Cloud-Kunden, die für die Steuerung ihrer Informationssicherheit auch IT-Revisoren einsetzen. Hier wird verdeutlicht, wie der C5 sowohl für die interne als auch die externe Revision in Form von Second-Party-Audits beim Cloud-Anbieter genutzt werden kann. IT-Revisionen allgemein und insbesondere im Cloud-Bereich auf der Basis des C5 stellen einen wichtigen Beitrag zur Informationssicherheit in der Wirtschaft dar. Wir danken der ISACA für die gemeinsame Arbeit an diesem Papier, um auch in diesem Bereich den C5 zu nutzen.

Horst Samsel
Abteilungsleiter »Beratung für Staat, Wirtschaft und Gesellschaft«
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Inhaltsverzeichnis

1 Einführung/Motivation

Cloud Computing entlässt Unternehmen nicht aus der Verantwortung für IT

Cloud Computing eröffnet vielversprechende Möglichkeiten, IT-basierte Geschäftsprozesse flexibel und effizient zu implementieren. Der Bezug skalierbarer Dienstleistungen ermöglicht es den Unternehmen, Anwendungen schneller in Betrieb zu nehmen und notwendige IT-Kapazitäten frühzeitiger den Marktforderungen anzupassen. Ebenso sind erhebliche Kosteneinsparungen durch damit verbundene Skalen- und Rationalisierungseffekte zu erzielen. Im Ergebnis stellen sich jedoch neue Fragen hinsichtlich Informationssicherheit und Compliance. Unternehmen sind in der Pflicht, diese Risiken umfassend zu bewerten und über den gesamten Lebenszyklus des Cloud-Dienstes zu überwachen.

Wie beim IT-Outsourcing stellt der externe Bezug von Dienstleistungen aus der Cloud eine spezielle Form der IT-Auslagerung dar. Aber auch hier gilt: »Prozesse und Services lassen sich auslagern, nicht aber die Verantwortung!« Als Cloud-Nutzer sind extern bezogene Cloud-Dienstleistungen als »eigene« Prozesse und Services zu betrachten und unterliegen damit denselben Anforderungen an die IT-Governance und Compliance wie die eigenen, internen Prozesse und Services. Diese goldene Regel ist auch Grundlage vieler branchenspezifischer Regularien zum IT-Outsourcing. Abhängig von Größe, Branche sowie von weiteren Faktoren verfügen viele Unternehmen über interne Überwachungs- und Kontrollinstanzen im Umfeld der IT-Governance. Entlang des Modells der drei Verteidigungslinien (»Three Lines of Defense Model«) sind für externe Cloud-Dienstleistungen die etablierten Security-Management-Funktionen (Second Line) sowie die Interne Revision (Third Line) von großer Bedeutung.

C5 bietet Orientierungshilfe für Audits durch den Cloud-Nutzer

2016 wurde seitens des Bundesamts für Sicherheit in der Informationstechnik (BSI) ein Anforderungskatalog für die Bewertung der Sicherheit von Cloud-Diensten (Cloud Computing Compliance Controls Catalogue, C5) veröffentlicht [BSI C5]. Auf Basis bereits heute anerkannter IT-Sicherheitsstandards (z. B. ISO/IEC 27001) sowie BSI-eigener Erweiterungen werden darin einheitliche Anforderungen an die Informationssicherheit von Cloud-Dienstleistungen formuliert. Ziel von C5 ist es, im Kontext der verschiedenen Zertifikate und Standards eine allgemein anerkannte Baseline für Cloud-Sicherheit zu definieren. Diese Anforderungen wurden in das internationale ISAE-3000-Prüfvorgehen eingebettet, sodass für Cloud-Anbieter gleichzeitig die Möglichkeit besteht, sich die Erfüllung der in C5 genannten Anforderungen mittels Prüfung durch Wirtschaftsprüfer testieren zu lassen. Das BSI behält nur die Anforderungen im Blick; die Prüfung und Testaterteilung erfolgt allein durch einen Wirtschaftsprüfer, ohne zusätzliche Aufsicht durch das BSI.

Für Cloud-Nutzer liegt es damit nahe, C5 auch als hilfreiche Orientierung und Grundlage für eigene Steuerungs- und Kontrollmaßnahmen der jeweiligen Second-Line-Funktionen (Security-Management) oder Prüfungen der Third-Line-Funktionen (Interne Revision) einzusetzen. Diese Maßnahmen sind beispielsweise dann sinnvoll und notwendig, wenn einer der folgenden Punkte vorliegt:

- Der Cloud-Anbieter verfügt nicht über ein C5-Testat einer Wirtschaftsprüfer- oder Prüfungsgesellschaft und ggf. vorhandene anderweitige Zertifikate (z. B. ISO/IEC 27001) des Anbieters werden als nicht ausreichend angesehen.
- Ein vorgelegtes C5-Prüftestat reicht aufgrund höherer eigener Anforderungen des Cloud-Nutzers entlang einer Risikobewertung nicht aus.

- Ein internes Auditprogramm des Cloud-Nutzers sieht generell eigene Prüfungen und Kontrollmaßnahmen beim Cloud-Anbieter vor. Gründe hierfür können z. B. industrie- und branchenspezifische Anforderungen sein (MaRisk[1] bei Finanzdienstleistern u.a.).
- Es liegen weitere regulatorische Anforderungen z. B. im Rahmen des Datenschutzes/der Auftragsdatenverarbeitung (ADV) vor. Hier ist es erforderlich, dass sich Cloud-Nutzer durch selbstständige Prüfungen von der Umsetzung bestimmter Maßnahmen des Cloud-Anbieters überzeugen.
- Mögliche Informationssicherheitsvorfälle haben sich ereignet, entweder beim Cloud-Anbieter generell oder im vom Kunden genutzten Cloud-System.

Darüber hinaus kann der C5-Anforderungskatalog auch bei der Beschaffung und Auswahl (Due Diligence) von Cloud-Diensten als wichtige Orientierungshilfe für die verantwortlichen First- und Second-Line-Funktionen des Cloud-Nutzers zum Einsatz kommen, z. B. als konkretes Anforderungsdokument bei der Sicherheitskonzeption. C5 ist nicht auf einzelne Cloud-Servicemodelle und -arten beschränkt und damit universell anwendbar[2].

1. Mindestanforderungen an das Risikomanagement der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).
2. Eine Cloud-Definition und Darstellung verschiedener Servicemodelle gibt es auch auf der Webseite des BSI: *https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html*.

2 Inhalte von C5

Der »Anforderungskatalog Cloud Computing – Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten« – oder kurz »C5« (für Cloud Computing Compliance Controls Catalogue) – ist ein Prüfstandard des Bundesamts für Sicherheit in der Informationstechnik (BSI). Der C5 definiert aus Sicht des BSI das Mindestniveau der Informationssicherheit für Cloud-Dienste und dessen Nachweis. Cloud-Dienste im professionellen Einsatz sollten nach Standpunkt des BSI zumindest dieses Niveau erfüllen.

Für die Entwicklung des C5 waren zwei Prämissen wesentlich:

- Er sollte den Konsens der Sicherheit von Cloud-Diensten abbilden, der sich bei Cloud-Anbietern und -Nutzern inzwischen herausgebildet hat. Vorhandene Standards und Mechanismen wurden in den C5 übernommen, sodass Cloud-Anbieter möglichst viel von ihren vorhandenen Sicherheitsmaßnahmen weiterhin verwenden können. Die Einbindung in ein bereits bestehendes Compliance-Management sollte mit minimalem Aufwand möglich sein.
- Der C5 bildet die Merkmale des Cloud Computing ab. So darf er die Dynamik des Cloud-Anbieters nicht behindern, muss für unterschiedliche Bereitstellungsmodelle nutzbar sein und ebenso auch Unterauftragnehmer berücksichtigen. Der C5 muss international anwendbar sein und damit der geografischen Verteilung von Cloud-Diensten Rechnung tragen.

Auch wenn der C5 somit ein Mindestsicherheitsniveau festlegt, entlässt er den Nutzer nicht aus der Verantwortung für seine eigenen Prozesse und Daten. Allerdings liefert er eine grundlegende und gute Entscheidungshilfe zur Auswahl eines Anbieters.

C5 besteht aus 3 Teilen: den Sicherheitsanforderungen, den Transparenzkriterien und den Anforderungen an einen belastbaren Nachweis der gemachten Angaben.

1. Die Sicherheitsanforderungen basieren auf gängigen Standards (ISO/IEC 27001, CSA Cloud Controls Matrix, AICPA Trust Services Principles and Criteria, ANSSI4 Référentiel Secure Cloud, IDW ERS FAIT 5, BSI IT-Grundschutz, BSI SaaS-Sicherheitsprofile) und wurden um Anforderungen des BSI ergänzt. Die resultierenden 114 Anforderungen sind thematisch in 17 Bereiche unterteilt (vgl. Abb. 2–1). Eine Referenzierung der Anforderungen des C5 auf die oben genannten Standards wurde ebenfalls veröffentlicht. Alle Anforderungen des C5 sind grundsätzlich zu erfüllen, solange sie anwendbar sind, und können nicht aus Risiko- oder anderen Abwägungen als obsolet gekennzeichnet oder nur teilweise erreicht werden. Darüber hinaus gibt es optionale Anforderungen, die ein höheres Niveau an die Vertraulichkeit und die Verfügbarkeit adressieren. Der Katalog lässt sich zusätzlich auch um eigene oder höhere Anforderungen ergänzen. Wie das Informationssicherheits-Managementsystem (ISMS) des Cloud-Anbieters genau auszusehen hat, schreibt der C5 nicht vor, empfiehlt aber, sich an bewährten Standards zu orientieren (z. B. ISO/IEC 27001).

Abb. 2–1 C5 umfasst 17 Kontrollbereiche mit 114 Anforderungen

2. Zu den Transparenzkriterien des C5 vergleichbare Anforderungen an die Offenlegung von Informationen gibt es in anderen Standards nur selten. Beim C5 muss der Cloud-Anbieter dem Nutzer wichtige Informationen – wie eine detaillierte Systembeschreibung –, alle Unterauftragnehmer, Datenlokalisation und Ermittlungsbefugnisse vorlegen. Denn dies sind wichtige Entscheidungsparameter für den Nutzer bei der Auswahl eines Cloud-Anbieters.
3. Auch beim Nachweis der Erfüllung der Kriterien durch Audits basiert der C5 auf etablierten Standards und Methoden und ergänzt diese im Einzelfall. Wirtschaftsprüfer führen Audits nach dem internationalen Standard ISAE 3000 bzw. dessen nationalen Umsetzungen durch. Der BSI-Katalog stellt noch einige zusätzliche Anforderungen, z. B. an die fachliche Qualifikation des Prüfteams. Die Berichte des C5 orientieren sich an SOC-2- oder ISAE-3402-Berichten, die inzwischen ebenfalls weit verbreitet sind. Der C5 fordert hier Typ-2-Berichte, die neben der Angemessenheit der Maßnahmen auch deren Wirksamkeit darlegen.

Die Abbildung 2–2 zeigt die drei Kernbereiche des C5: Sicherheitsanforderungen, Nachweis- und Transparenzkriterien. Etablierte Standards für Sicherheitsanforderungen und Audit werden vom C5 ergänzt oder geschärft.

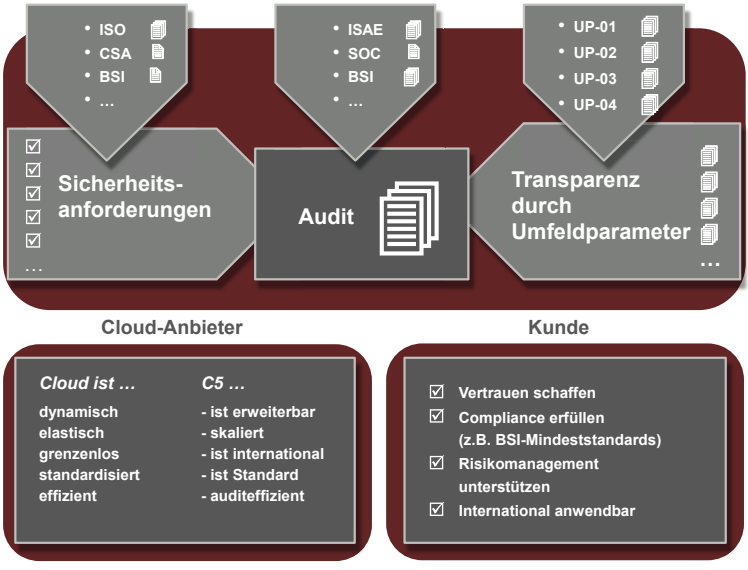

Abb. 2–2 Kernbestandteile des C5

3 Anwendung von C5 durch die Interne Revision

3.1 Prüfungen beim Cloud-Dienstleister als Second-Party-Audit

Die klassische Form der Internen Revision ist das First-Party-Audit, also Prüfungen im eigenen Unternehmen. Die Prüfungsleistung wird oft auch als dritte Verteidigungslinie des Unternehmens angesehen und unabhängig vom operativen Betrieb und Security- und Compliance-Management erbracht. Bestandteil ist hier grundsätzlich eine Berichterstattung, die idealerweise die Geschäftsleitung direkt anspricht und erreicht.

Durch die Einführung von Cloud Computing und die damit einhergehende Auslagerung von Leistungen erlangt das sogenannte Second-Party-Audit ebenfalls zunehmende Bedeutung in der Praxis der Internen Revision. Bei diesem Audit erstreckt sich die Prüfung nicht nur auf das eigene Unternehmen, sondern auch auf den externen Cloud-Dienstleister (vgl. Abb. 3–1). Ziel ist es, festzustellen, ob der Dienstleister die Leistungen in der notwendigen Qualität, Sicherheit und Zuverlässigkeit erbringt, wie sie im eigenen Unternehmen gefordert werden. Voraussetzung für solche Prüfungen ist u.a. ein vertragliches Prüfungsrecht bei Abschluss des Cloud-Computing-Vertrags.

Der C5 des BSI bildet eine gute Grundlage für die Durchführung von Second-Party-Audits durch die Interne Revision, da er insbesondere im eigenen Kapitel 5 konkrete Anforderungsbereiche an den Cloud-Anbieter definiert, die dann in der Revisionsprüfung mit herangezogen werden können. Zudem müssen nach C5 in Kapitel 4 Cloud-Anbieter auch relevante Umfeldparameter (z. B. Standorte der Datenverarbeitung und relevante Subdienstleister) transparent machen. Damit hat die Interne Revision einen guten Gesamtüberblick über die konkrete Auslagerungssituation. Im Einzelnen sind dies folgende Punkte:

- UP-01 Systembeschreibung,
- UP-02 Gerichtsbarkeit und Lokationen der Datenspeicherung, -verarbeitung und -sicherung,
- UP-03 Offenbarungs- und Ermittlungsbefugnisse sowie
- UP-04 Zertifizierungen.

Liegt ein Prüftestat einer externen Prüfungsgesellschaft nach C5 vor, kann die Interne Revision die dort dokumentierten externen Prüfungserkenntnisse im Rahmen der Second-Party-Prüfungen berücksichtigen und würdigen. Dabei sollte beachtet werden, ob eine Testierung nach Typ 1 oder Typ 2 vorliegt. Nur im letzteren Fall wurde auch die Wirksamkeit der implementierten Maßnahmen durch die ausstellende Stelle überprüft. Ist der Anbieter bereit, auch die dem Testat zugrunde liegende Dokumentation offenzulegen, wie z. B. die nach Abschnitt 3.3.2 zu erstellende Systembeschreibung, kann diese auch eine gute Basis für weitere Prüfungen bilden.

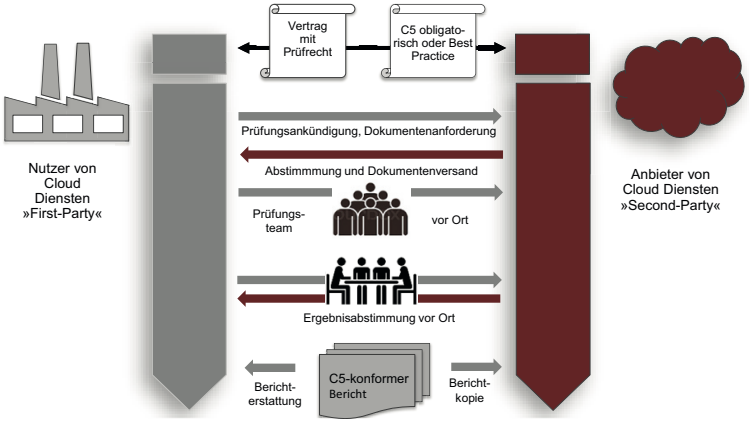

Abb. 3–1 Prozessablauf eines Second-Party-Audits im Cloud-Umfeld

3.2 Anwendbare Prüfungsstandards

Der C5-Anforderungskatalog des BSI definiert in Kapitel 3.2 konkrete Prüfungsstandards für die Auditierung des Cloud-Dienstleisters und für die Ausstellung eines Testats durch eine externe Prüfungsgesellschaft. Dies gewährleistet im Besonderen die Unabhängigkeit der externen Prüfer und die Verbindlichkeit und Nachvollziehbarkeit der Prüfungsnachweise.

Bei der Internen Revision ist es dagegen jedem Unternehmen freigestellt, eine Auditierung entlang eines geeigneten Revisionsstandards vorzunehmen. Je nach Branche liegen hierfür auch gesetzliche Gründe vor. Prüfungen der Internen Revision im Bereich der Informationssysteme unterscheiden in der Regel nicht, ob es sich um die eigene Unternehmens-IT oder von Dritten erbrachte Cloud-Dienstleistungen handelt. Grundlegende Anforderungen und Standards, wie z. B. die Unabhängigkeit der Revisoren, sind auch bei Cloud-Dienstleistungen in gleicher Weise zu beachten. Es empfiehlt sich daher, etablierte und standardisierte Verfahren einzusetzen. Die im nachfolgenden beschriebenen ITAF-Prüfungsstandards stellen solch ein geeignetes Verfahren dar.

3.3 Information Technology Assurance Framework als Prüfungsgrundlage

Das »Information Technology Assurance Framework« (ITAF) ist ein umfassendes Referenzmodell der ISACA, das grundlegende Orientierungshilfen für IT-Prüfungsaufträge definiert. Neben Anforderungen an Sorgfalt, Durchführung und Berichterstattung enthält es auch Vorgaben für Verantwortlichkeiten und Qualifikationen des Prüfers. Es kann sehr gut als Basis für Prüfungen durch einen internen IT-Auditor im Bereich Cloud Computing herangezogen werden. ITAF setzt sich aus Auditstandards und Auditleitlinien (Guidelines) zusammen. Die Standards bestehen aus knapp formulierten Statements, die grundlegende Anforderungen definieren. Jedes Statement wird durch eine Leitlinie ergänzt, die weitere Unterstützung für die Durchführung des Audits liefert und Bezüge zu den COBIT-Governance-Prozessen herstellt.

Die Prüfung von Cloud-Services nach ITAF stellt den Prüfer aber vor verschiedene Cloud-spezifische Herausforderungen und Schwierigkeiten, die im Rahmen einer internen Prüfung in der Regel nicht auftreten. Tabelle 3–1 gibt eine Übersicht über die einzelnen ITAF-Standards und zu beachtende Besonderheiten bei Cloud Computing. Mit dem »IT Audit and Assurance Program for Cloud Computing« hat die ISACA im Jahr 2014 auch schon auf solche Cloud-spezifischen Ausprägungen und Anforderungen für Prüfhandlungen innerhalb von COBIT 5 hingewiesen [ISACA 2014].

ITAF-Standards	Ergänzende Hinweise für die Anwendung bei Cloud Computing
Allgemein	
1001 - Audit Charter	Das Audit Charter oder die Geschäftsordnung der Internen Revision müssen eine Prüfung der Cloud-Dienste extern bei Vertragspartnern zulassen. Es dürfen keine einschränkenden Formulierungen Zweifel daran entstehen lassen, dass die Interne Revision auch bei Vertragspartnern umfänglich prüfen kann.
1002 - Organisatorische Unabhängigkeit	-
1003 - Persönliche Unabhängigkeit	Mitarbeiter/innen der Internen Revision, die persönliche oder geschäftliche Beziehungen zu externen Cloud-Anbietern unterhalten, sollten nicht mit einem Prüfungsauftrag betraut werden.
1004 - Hinreichende Durchführbarkeit	Im Vertrag mit dem Anbieter muss sichergestellt werden, dass ausreichende Prüfrechte durch den Nutzer vorhanden sind und beim Cloud-Anbieter ausreichende Ressourcen bei der Prüfung zur Verfügung stehen.
1005 - Berufsübliche Sorgfalt	-
1006 - Expertise	Die technische und rechtliche Konstruktion von Cloud-Diensten muss fachlich angemessen durch das Prüfteam beurteilt werden können. Dazu sollten grundlegende Kenntnisse der bei Cloud Computing angewandten Technologien und Serviceprozesse vorhanden sein.

→

1007 - Aussagen	-
1008 - Kriterien	Relevante Kriterien für die Prüfung sollten sich am C5-Anforderungskatalog orientieren. Erweiterungen auf Grundlage der eigenen Risikosituation sind jederzeit möglich.
Durchführung	
1201 - Auftragsplanung	Bei der Planung der Prüfungsdurchführung ist eine frühzeitige Abstimmung und Koordination mit dem Cloud-Anbieter empfehlenswert.
1202 - Risikoorientierte Planung	Das Risikobeurteilungsverfahren der Internen Revision sollte in der Lage sein, für Cloud-Dienste eine angemessene Risikobewertung vorzunehmen.
1203 - Durchführung und Überwachung	Zu den Feststellungen und deren Nachweise in der Prüfung gehören ggf. auch Prüfungen der Subdienstleister vor Ort. Entsprechende Prüfungsrechte bei Subdienstleistern sollten vertraglich vereinbart werden.
1204 - Wesentlichkeit	-
1205 - Nachweise	-
1206 - Verwendung der Ergebnisse anderer Sachverständiger	Das Vorliegen eines BSI-C5-Testats durch einen Wirtschaftsprüfer sowie andere einschlägige Beurteilungen (z. B. Zertifikat nach ISO/IEC 27001/27017) müssen angemessen bei der Prüfung berücksichtigt werden und können ggf. den Umfang der eigenen Prüfhandlungen reduzieren.
1207 - Unregelmäßigkeiten und gesetzeswidrige Handlungen	Strafbare Handlungen im Cloud-Umfeld (z. B. Verstöße gegen §§ 202a-d, §§ 303a und b sowie § 270 StGB) muss der Prüfer zur Kenntnis bringen.
Berichterstattung	
1401 - Berichterstattung	Die Kooperation und Mitwirkung bei der Beseitigung von Mängeln ist generell vertraglich zu regeln.
1402 - Nachschau	-

Tab. 3–1 ITAF-Anforderungen und Cloud-spezifische Besonderheiten

3.4 Cloud-spezifische Herausforderungen und Rahmenbedingungen

Auditpflicht und Auditrecht

Cloud-Nutzer haben in verschiedenen Szenarien die Pflicht, den Cloud-Anbieter zu auditieren. Hierzu zählen z. B. Szenarien in der Finanzbranche, die den Anforderungen des MaRisk unterliegen. Cloud-Anbieter sind hingehen nicht grundsätzlich verpflichtet, sich auditieren zu lassen. Da aber immer mehr Regularien dem Cloud-Nutzer eine Auditpflicht auferlegen und Cloud-Anbieter ihren Service attraktiv halten wollen, sind auch Cloud-Anbieter zunehmend bereit, dem Cloud-Nutzer ein Auditrecht vertraglich einzuräumen. Weiterhin enthalten z. B. die EU-Datenschutz-Standardvertragsklauseln ein Auditrecht, das bei der Verarbeitung personenbezogener Daten außerhalb des europäischen Raumes anzuwenden ist und von verschiedenen Cloud-Anbietern teils standardmäßig oder auf Anfrage in die Verträge aufgenommen wird. Ähnliches gilt beim Abschluss eines Vertrags zur Auftragsdatenverarbeitung nach dem Bundesdatenschutzgesetz.

Eingeschränkte Auditrechte

Unter Umständen hat der Cloud-Nutzer keine oder nur eingeschränkte Auditrechte beim Anbieter. Die Einschränkung für Vor-Ort-Audits kann eine große Spannbreite aufweisen:

- Der Anbieter bietet grundsätzlich keine Möglichkeit zur Durchführung von Vor-Ort-Audits.
- Es besteht die Möglichkeit zu Vor-Ort-Audits mit zeitlichen Einschränkungen (z. B. werden Audits auf eine gewisse Anzahl von Tagen pro Jahr limitiert).
- Vor-Ort-Audits sind möglich, aber nur für Sachverhalte, die nicht bereits in den Zertifizierungen und Compliance-Reports des Cloud-Anbieters durch dessen Third-Party-Auditoren abgedeckt sind.

Cloud-Nutzer sollten daher schon vor Vertragsabschluss folgende vorausschauende und kompensierende Maßnahmen erwägen:

- Die Aufnahme des Auditrechts in die Auswahlkriterien für Cloud-Anbieter
- Die Vereinbarung eines Vor-Ort-Auditrechts im Vertrag
- Vor Vertragsabschluss sind auch schon mögliche Erweiterungen der in der Cloud-Lösung verarbeiteten Daten zu antizipieren. So können sich beispielsweise durch eine spätere Hinzunahme der Verarbeitung von personenbezogenen Daten oder Finanzdaten die Anforderungen an Audits grundlegend ändern.
- Gegebenenfalls sind vertragliche Auditrechte nachzuverhandeln, falls der ursprüngliche Vertrag diese nicht angemessen enthält.
- Eine Prüfung, inwieweit die Cloud-Lösung Remote-Zugänge anbietet, um die Audits teilweise oder komplett über einen externen Zugriff durchzuführen (z. B. Benutzerverwaltung, Berechtigungen und Änderungsmanagement).
- Sind eigene Audits nicht zwingend vorgegeben, kann mit einem risikobasierten Ansatz auf vorhandene Auditergebnisse in Third-Party-Zertifizierungen, Testaten und Compliance-Reports des Cloud-Anbieters zurückgegriffen werden (siehe auch Anforderung COM-03 des C5).

Auditrechte bei Subdienstleistern

Es ist zu empfehlen, bei allen Vertragsvereinbarungen das Auditrecht auch auf bereits existierende und potenziell später hinzukommende Unterauftragnehmer auszudehnen. Sonst kann ggf. die im Auftrag des Anbieters durchgeführte Datenverarbeitung nicht auditiert werden. Falls der Cloud-Anbieter C5 erfüllt, ist sichergestellt, dass er sich selbst ausreichende Auditrechte bei seinem Unterauftragnehmer hat einräumen lassen (siehe DLL-01 und DLL-02 des C5).

Eingeschränkter Auditumfang durch unvollständige Mandantentrennung

Mandantenübergreifend genutzte Infrastruktur kann besonders bei Public Clouds den möglichen Prüfungsumfang beim Anbieter stark einschränken, da sonst der Anbieter die Sicherheit der Daten anderer Nutzer gefährden würde.

Erhöhte Komplexität

Die Architektur und Komplexität der vom Cloud-Anbieter verwalteten IT unterscheiden sich oft sehr von der im Unternehmen selbst genutzten und kann Prüfer ohne Cloud-Kenntnisse möglicherweise überfordern. Best Practices und Erfahrungen aus den internen Prüfungen lassen sich meist nur sehr begrenzt auf den externen Anbieter übertragen. Der C5 fordert jedoch eine aussagekräftige Systembeschreibung (siehe Umfeldparameter UP-01), mit der man sich einen strukturierten Überblick über den Cloud-Dienst verschaffen kann.

Hohe Dynamik des Cloud Computing

Cloud-Computing-Infrastrukturen weisen oft eine sehr hohe Dynamik auf. So kann die Datenverarbeitung unbemerkt vom Nutzer auf andere Komponenten oder Orte verlagert werden, unter Umständen sogar über Regionen oder Landesgrenzen hinaus. Dabei können sich Technologien, Prozesse und Verantwortungen teilweise erheblich ändern. Ein Cloud-Anbieter, der »C5-compliant« ist, muss sich an die vom Cloud-Nutzer festgelegten Standorte der Datenverarbeitung halten (siehe RB-03 des C5). Über relevante Änderungen des Service muss der Cloud-Nutzer gemäß der C5-Anforderung BEI-03 benachrichtigt werden, wenn dies vertraglich vereinbart wurde. So kann nachvollzogen werden, ob und welche Änderungen es gab.

Umgang mit personenbezogenen Daten

Vertragliche Regelungen zu den anzuwendenden Datenschutzstandards müssen ein angemessenes Sicherheits- und Datenschutzniveau beim Cloud-Anbieter sicherstellen, sobald personenbezogene Daten verarbeitet werden. Besondere Regelungen müssen vereinbart werden, wenn personenbezogene Daten in Nicht-EU-Staaten transferiert werden. Die Datenschutzverordnungen der EU unterscheiden grundsätzlich zwei Szenarien: »Controller zu Controller« oder »Controller zu Processor«. Beide Fälle räumen dem Sender der Daten ein Auditrecht beim Empfänger der Daten ein. Einzelne Cloud-Anbieter können sich aber darin unterscheiden, wie sie diese Anforderungen interpretieren und sich bei ihren Vertragsbedingungen an den von der EU geforderten Vertragsklauseln orientieren.

3.5 Qualifikation des Prüfers

Im Gegensatz zu den durch Wirtschaftsprüfer durchgeführten Audits nach ISAE 3402 benötigen interne Auditoren keine bestimmten Zertifizierungen oder Qualifikationsnachweise. Dennoch sollte auf eine ausreichende Qualifikation der Prüfer geachtet werden. Diese sollten neben der Kenntnis der Anforderungen an die Prüfprozesse auch grundlegendes Wissen im Bereich Informationssicherheit und Risikomanagement besitzen. Die benötigten Qualifikationen können durch Schulungen und Zertifizierungen erworben bzw. nachgewiesen werden, z. B. von DIIR, ISACA oder (ISC)^2. Für Prüfer empfehlenswerte Zertifikate sind u.a. die ISACA-Zertifikate CISA, CISM oder CRISC. Da Cloud Computing auch webbasierte Technologien stark nutzt, sollte ein Prüfer von Cloud-Diensten insbesondere auch Grundlagenkenntnisse im Bereich Webservices und Web-Security haben.

4 Anwendung von C5 im Informationssicherheitsmanagement

Damit Unternehmen die Vorteile von Cloud Computing optimal nutzen können, müssen Governance- und Managementprozesse im Unternehmen an die geänderten Bedingungen angepasst werden. Weil sich mit der Einführung von Cloud Computing die Möglichkeit der direkten betrieblichen Einflussnahme auf IT-Systeme, Anwendungen und Prozesse reduziert, ist darauf zu achten, dass Informationssicherheit und Compliance im genutzten Governance-Modell und in den Prüfungsszenarien weiterhin ausreichend berücksichtigt werden. Die im Rahmen von C5 definierten Mindestanforderungen können dem Sicherheitsmanagement über alle Phasen des Lebenszyklus eines Cloud-Dienstes hinweg wichtige Unterstützung liefern. Anhand des ITIL-Lebenszyklusmodells für IT-Services wird dies in den folgenden Abschnitten beispielhaft beschrieben. Die Aussagen gelten aber auch für andere Governance-Modelle wie z. B. COBIT. Am Beispiel der für die Einführung eines Cloud-Service zu durchlaufenden Phasen und zu erstellenden Dokumente sind diese Prozessschritte in Abbildung 4–1 schematisch dargestellt. In jeder Phase existieren Aufgaben, bei denen C5 wertvolle Unterstützung liefern kann. Einige konkrete Beispiele sind in Tabelle 4–1 aufgeführt.

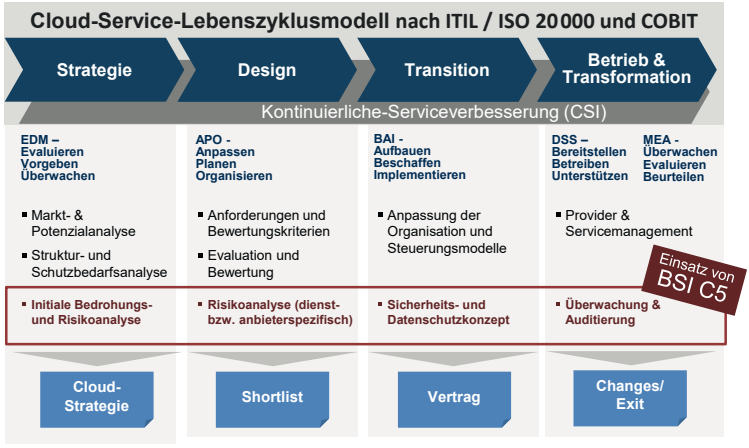

Abb. 4–1 Lebenszyklusphasen eines Service nach ITIL- und COBIT-Prozessen, die bei der Nutzung von Cloud Computing betrachtet werden müssen (nach [ITIL V3], [ISO 20000-11], [ISACA 2012]). In allen Prozessschritten kann C5 als Unterstützung herangezogen werden.

Phase 1: Analyse und Strategieentwicklung

Vor dem Einsatz von Cloud Computing müssen Unternehmen den Markt und die technologischen Entwicklungen im Bereich Cloud Computing analysieren und in ihrer IT-Strategie berücksichtigen. Hierzu gehören auch Aussagen, nach welchen Standards und Betriebsmodellen man die IT ausrichten will. Selbstverständlich sind auch die Bereiche Informationssicherheit und Datenschutz Teil dessen. C5 bietet hier die Möglichkeit, Informationssicherheit über verschiedene Standards und Frameworks hinweg konsistent zu adressieren.

Phase 2: Servicedesign und Auswahl eines Anbieters

Die Auswahl einer Servicearchitektur (z. B. Public, Private oder Hybrid Cloud) muss unter Berücksichtigung der damit verbundenen Risiken für die Informationsverarbeitung und ggf. vorhandener rechtlicher Aspekte erfolgen. Dazu werden üblicherweise, in Form eines »RFI« oder »RFP« (Request For Information/Proposal), die erforderlichen Anforderungen in strukturierter und verbindlicher Weise vom Provider abgefragt. C5 kann hier als solide Grundlage für die Formulierung dieser Anforderungen herangezogen werden.

Phase 3: Transition

Die Transition-Phase erstreckt sich von Vertragsverhandlungen und Vertragsabschluss bis hin zur abgeschlossenen Auslagerung. Parallel zum Auslagerungsprozess sollte in dieser Phase ein detailliertes Sicherheits- und Datenschutzkonzept erstellt werden, das sowohl die ausgelagerten Dienstleistungen als auch die im Unternehmen verbleibenden Komponenten umfasst. Wurden die Dienste nach dem im C5 definierten Kriterienkatalog eingekauft bzw. entworfen, kann man sich hier direkt auf die dort beschriebenen Maßnahmen stützen. Die bereits definierte Korrelation zu ISO/IEC 27001 erlaubt dabei die direkte Integration in ein nach dieser ISO-Norm ausgerichtetes Informationssicherheits-Managementsystem und IT-Risikomanagement.

Phase 4: Betrieb und Transformation

Während der Betriebsphase ist sicherzustellen, dass sicherheitsrelevante Prozesse implementiert sind und nachgewiesenermaßen funktionieren. Dazu gehört es – unabhängig von den in den vorangegangenen Abschnitten beschriebenen Audits durch die Revision –, auch Mechanismen zu implementieren, mit denen die Sicherheit des (Cloud-)Dienstes überwacht werden kann. Bei der Konzeption und Implementierung dieser Funktionen können die technischen Anforderungen des C5-Katalogs ebenfalls als Grundlage herangezogen werden.

Phase 5: Kontinuierliche Serviceverbesserung (CSI)

ITIL umfasst auch den kontinuierlichen Service-Verbesserungsprozess (CSI = Continuous Service Improvement). Ziel des CSI-Prozesses ist es, mit Methoden des Qualitätsmanagements die Effektivität und Effizienz von IT-Prozessen und -Services fortlaufend zu verbessern. In Bezug auf Sicherheit kann die Umsetzung und Einhaltung der Anforderungen des C5 z. B. eine wichtige Kenngröße bilden, mit der der aktuelle Stand der Sicherheit erfasst wird. Ist der Cloud-Dienst in wichtigen Punkten nicht compliant mit C5, sollte überlegt werden, ob das entstehende Risiko auf Nutzerseite durch kompensierende Maßnahmen reduziert werden kann.

Phase	Cloud-Nutzer	Cloud-Anbieter
Strategie	Compliance mit C5 als Kriterium für Cloud-Services fordern, ggf. mit Hinweisen auf besonders zu beachtende Umfeldparameter	Einführung von C5 anstelle anderer bisher angewendeter Standards zur internen und externen Bewertung der Compliance
Design	Auswahl von Cloud-Services anhand des C5	C5-konforme Auslegung der Services bereits in der Design-Phase
Transition	Integration der implementierten C5-Maßnahmen in das ISMS	Durchführung interner Audits gegen C5 bei der Serviceimplementierung
Betrieb & Transformation	Auswertung der C5-Compliance von genutzten Cloud-Services	Regelmäßige interne Audits gegen C5
Kontinuierliche Verbesserung	Definition und Implementierung kompensierender Maßnahmen auf Nutzerseite bei eingeschränkter C5-Compliance	Messen und ggf. Erhöhen des Grades an Compliance zu C5

Tab. 4–1 Beispiele für die Nutzung des C5 durch Cloud-Nutzer und Cloud-Anbieter

5 Zusammenfassung und Ausblick

Die in C5 des BSI enthaltenen Mindestanforderungen können sowohl von Cloud-Nutzern als auch Cloud-Anbietern gleichermaßen als Rahmenvorgabe und Orientierung angewendet werden. Dabei ist es nicht erforderlich, dass der betrachtete Dienstleister ein C5-Testat besitzt oder anstrebt.

Der Internen Revision liefert der Kriterienkatalog wichtige Inhalte für die Prüfungen beim Cloud-Dienstleister im Rahmen von Second-Party-Audits. Statt des von Wirtschaftsprüfern eingesetzten ISAE-3000-Frameworks können diese Audits z. B. auch nach der von ISACA empfohlenen ITAF-Methodik durchgeführt werden. Hierzu muss im Vorfeld durch entsprechende vertragliche Regelungen die Grundlage für solche Audits geschaffen werden.

Auch im Informationssicherheitsmanagement kann C5 in den verschiedenen Lebenszyklusphasen eines Cloud-Service herangezogen und z. B. bei Strategieentwicklung, Servicedesign, Vertragsabschluss und während des laufenden Betriebs angewendet werden.

Da C5 noch relativ neu ist, stehen umfassende Auditerfahrungen noch aus. Wenn sich das Konzept eines generell anwendbaren Kriterienkatalogs mit Mindestanforderungen bei Cloud Computing in der Praxis bewährt, wäre dies auch ein möglicher Blueprint für andere IT-Technologien, wie z. B. Industrial Security und Internet of Things, bei denen allgemein anerkannte Prüfkriterien noch nicht existieren und erst entwickelt werden müssen.

6 Quellenverzeichnis

[BSI C5] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anforderungskatalog Cloud Computing (C5). Bundesamt für Sicherheit in der Informationstechnik, 2016; *https://www.bsi.bund.de/C5*.

[ISACA 2012] ISACA: COBIT 5 – Rahmenwerk für die Governance und das Management der unternehmensweiten IT. ISACA International, 2012; *http://www.isaca.org/COBIT/*.

[ISACA 2014] ISACA: IT Audit and Assurance Program for Cloud Computing. ISACA International, 2014, abrufbar unter: *http://www.isaca.org/Knowledge-Center/*.

[ISO 20000-11] ISO: ISO/IEC TR 20000-11:2015 Information technology – Service management – Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®, 2015.

[ITAF 2014] Information Technology Assurance Framework (ITAF™): Rahmenwerk der Berufspraktiken für die IT-Prüfung. 3. Ausgabe, ISACA, 2014; *http://www.isaca.org/Knowledge-Center/Research/Documents/ITAF-3rd-Edition_fmk_Ger_0916.pdf*.

[ITIL V3] Information Technology Infrastructure Library (ITIL) Version 3, Axelos; *https://www.axelos.com/best-practice-solutions/itil/itil-ublications*.

ISACA Germany Chapter e.V.
Oberwallstrasse 24
10117 Berlin

www.isaca.de
info@isaca.de