Naybzadeh, Milan

Working Paper

Standards und Zertifizierungen für Cloud-Services

SIMAT Arbeitspapiere, No. 13-21-039

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Naybzadeh, Milan (2021) : Standards und Zertifizierungen für Cloud-Services, SIMAT Arbeitspapiere, No. 13-21-039, Hochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund

This Version is available at:
https://hdl.handle.net/10419/234595

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 13-21-039

Standards und Zertifizierungen für Cloud-Services

Milan Naybzadeh

Hochschule Stralsund
SIMAT Stralsund Information Management Team

Mai 2021

ISSN 1868-064X

Naybzadeh, Milan: Standards und Zertifizierungen für Cloud-Services. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: Hochschule Stralsund, SIMAT Stralsund Information Management Team, 2021 (SIMAT AP, 13 (2021), 39), ISSN 1868-064X

Impressum

Hochschule Stralsund
Zur Schwedenschanze 15
18435 Stralsund
www.hochschule-stralsund.de

Herausgeber
Prof. Dr. Michael Klotz
Fakultät für Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@hochschule-stralsund.de

Print
Digitaldruck: www.dokuteam-x.de
Behrndt & Herud GmbH
Anklamer Straße 98
17489 Greifswald

Autor

Milan Naybzadeh hat einen Bachelor-Abschluss in Informationsrecht (Bachelor of Laws) an der Hochschule Darmstadt und einen Master-Abschluss in IT-Governance, Risk and Compliance-Management (Master of Science) an der Hochschule Albstadt-Sigmaringen erlangt. Er hat als Netzwerkbetreuer, Datenschutz-Auditor und IT-Sicherheitsbeauftragter gearbeitet und ist heute IT-Compliance-Manager bei der ADACOR Hosting GmbH.

Standards und Zertifizierungen für Cloud-Services

Naybzadeh, Milan[1]

Zusammenfassung: Bei der Nutzung von Cloud-Services besteht für Kunden das Risiko des Kontrollverlusts, da die Überwachung der Funktionalität der Cloud-Services überwiegend dem Cloud-Service-Anbieter obliegt und deshalb vom Cloud-Service-Kunden nur eingeschränkt verfolgt, überwacht und beeinflusst werden kann. Zertifizierungen können in dieser Situation Vertrauen schaffen, indem sie die Transparenz der Leistungserbringung erhöhen. Da eine Vielzahl von Zertifizierungen existiert, die jeweils verschiedene Schwerpunkte setzen, können diese von Kunden in ihrem jeweiligen Kontext unterschiedlich bewertet werden. Voraussetzung hierfür ist aber die Kenntnis der verschiedenen Zertifizierungen. Dieses Arbeitspapier gibt einen Überblick über die Zertifizierungsmöglichkeiten für Cloud-Service-Anbieter und beschreibt diese. Die Auswahl der Cloud-Service-Anbieter ist im Rahmen einer Praxisstudie entstanden und zeigt vor allem Zertifizierungen auf, die bereits in der Praxis bei Cloud-Service-Anbietern Anwendung finden.

Gliederung

[1] Der Autor ist erreichbar auf Xing über https://www.xing.com/profile/Milan_Naybzadeh/ und auf LinkedIn über https://de.linkedin.com/in/milan-naybzadeh-b4281b70 .

Schlüsselwörter: Cloud-Services – IT-Normen – IT-Standards – Zertifizierung – ISO – IEC – NIST

JEL-Klassifikation: L15, L86, M19, M49

Vorwort des Herausgebers

Das Outsourcing weiter Teile der IT-Infrastruktur und verbundener IT-Services ist einer der derzeitigen Hauptstrategien für einen effektiven und effizienten IT-Betrieb. Die Verlagerung von Aufgaben bedeutet aber nie eine Verlagerung der Verantwortung für Steuerung und Überwachung. Sowohl bei der Auswahl von Cloud-Service-Anbietern als auch bei der Überwachung der von diesen zu erbringenden Cloud-Services können Zertifizierungen eine wichtige Rolle spielen. Sie sollten gleichsam die Basis des Nachweises der Erfüllung von Sorgfaltspflichten im IT-Management darstellen.

Das vorliegende, von Milan Naybzadeh verfasste Arbeitspapier präsentiert in systematischer Weise Zertifizierungen im Bereich des Angebotes von Cloud-Services. Auch hier ist mittlerweile nur schwer eine Übersicht zu erlangen. Es ist das Verdienst des Autors, dass er basierend auf einer empirischen Studie eine praxisnahe Auswahl trifft, die der Vorselektion in einer realen Entscheidungssituation dienen kann.

Hinsichtlich der Regelwerke der IT-Compliance handelt es sich bei den hier betrachteten, den Zertifizierungen zugrundliegenden Dokumenten um IT-Normen und -Standards. Insofern gliedert sich vorliegende Ausarbeitung in die Abfolge der Arbeitspapiere zu den Regelwerken der IT-Compliance – Klassifikation und Übersicht (AP Nr. 11, 20 und 24) ein und ergänzt die bisherigen Übersichten über IT-Gesetze und IT-Normen.

Prof. Dr. Michael Klotz

Tabellenverzeichnis

Abkürzungsverzeichnis

AG	Aktiengesellschaft
AICPA	Association of International Certified Professional Accountants
AO	Assessment Organization
a.s.b.l	Association sans but lucratif (Vereinigung ohne Gewinnerzielungsabsicht)
BMWi	Bundesministeriums für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informations-technik (BSI-Gesetz)
C5	Cloud Computing Compliance Criteria Catalogue des Bundesamts für Sicherheit in der Informationspolitik
CIS	Center for Internet Security
CSA STAR	Cloud Security Alliance - Security Trust Assurance and Risk
CSF	Cyber Security Framework
DAkkS	Deutsche Akkreditierungsstelle
DACH	Zusammenfassung deutschsprachiger Raum: Deutschland (D), Österreich (A), Schweiz (CH)
EN	Europäische Norm
FedRAMP	Federal Risk and Authorization Management-Programm
HITRUST	Health Information Trust Alliance
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
IDW PS	Prüfstandard des Instituts der Wirtschaftsprüfer in Deutschland
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
IT	Informationstechnik
ITSMS	IT-Service-Managementsystem
NIST	National Institute of Standards and Technology
PaaS	Plattform as a Service
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	PCI Security Standards Council
SA	Star Audit
SaaS	Software as a Service

SAR	Security Assessment Report
SAQ	Self-Assessment Questionnaire
SOC	Service Organization Controls
SP	Special Publication
SSP	Systemsicherheitsplan
SQ	Sicherheitstechnische Qualifizierung
TISAX	Trusted Information Security Assessment Exchange
TR	Technischer Report
TPS	Trusted Product Security
TSC	Trust Service Principles
TSS	Trusted Site Security
TÜV	Technischer Überwachungsverein
TÜViT	TÜV Informationstechnik GmbH
USA	Vereinigte Staaten von Amerika
VDA ISA	Katalog zum Information Security Assessment des Verbands der Automobilindustrie
WP	Wirtschaftsprüfer

1. Einleitung

Cloud Computing und Cloud Services

Cloud-Computing bietet eine bedarfsgerechte und flexible Bereitstellung und Nutzung von IT-Ressourcen. Dabei umschreibt der Begriff eine Art der Leistungserbringung, bei denen die IT-Ressourcen als Services zur Verfügung gestellt werden.[2]

Einsatz von Zertifizierungen

Bei der Nutzung von Cloud-Services besteht für Kunden das Risiko des Kontrollverlusts, da die Überwachung der Funktionalität der Cloud-Services überwiegend dem Cloud-Service-Anbieter obliegt und deshalb vom Cloud-Service-Kunden nur eingeschränkt verfolgt und beeinflusst werden kann.[3] Zertifizierungen können hierbei Vertrauen schaffen, indem sie die Transparenz erhöhen.[4] Da eine Vielzahl von Zertifizierungen existiert, die verschiedene Schwerpunkte setzen, können diese von Kunden in ihrem jeweiligen Kontext unterschiedlich bewertet werden.[5]

Ausblick

Im Folgenden werden Zertifizierungen benannt und systematisch dargestellt. Die Auswahl und Aufteilung ist im Rahmen einer Praxisstudie entstanden und zeigt vor allem Zertifizierungen auf, die bereits in der Praxis bei Cloud-Service-Anbietern Anwendung finden.

2. Definition Zertifizierung

Ungenauer Begriff

Zunächst bedarf es eines Verständnisses, was eine „Zertifizierung“ ausmacht, da verschiedene Formen und Ausprägungen vorzufinden sind.

Herleitung

Bei Betrachtung von Praxis und Literatur findet sich zunächst eine uneinheitliche Verwendung des Begriffs „Zertifizierungen“. Es wird meist von einem Verfahren gesprochen, bei dem eine unabhängige Partei formal und nachvollziehbar für Außenstehende bewertet, ob ein Produkt, ein Prozess, ein System oder eine Person konform zu definierten Anforderungen ist.[6] Die Ausgestaltung eines Zertifizierungsverfahrens ist aber nicht einheitlich vorgegeben.[7] Im weiteren Sinne handelt es sich bei einer Zertifizierung also um

[2] Vgl. National Institute of Standards and Technology, 2011.
[3] Vgl. Marston, et al., 2011.
[4] Vgl. Sunyaev & Schneider, 2013; Lang, et al., 2018, Behringer & Passarge, 2020, S. 265.
[5] Vgl. Booz & Company, 2012; Schneider, et al., 2014.
[6] Vgl. Braunweiler, et al., 2015, S.9; Akerlof, 1979, S. 488; Lang, et al., 2018b, p. S. 61 ff.; Glossar der Deutschen Akkreditierungsstelle (https://www.dakks.de/content/glossar), zuletzt aufgerufen am 03.01.2020;
[7] Vgl. Traudes, 2017, S. 159.

die Beschreibung eines Verfahrens zur Überprüfung der Einhaltung vorgegebener Anforderungen, inklusive eines für Dritte nachvollziehbaren Ergebnisdokuments.

Regelwerke als Grundlage

Vorgegebene Anforderungen werden in Regelwerken niedergeschrieben.[8] Im Rahmen der zugrundeliegenden Studie stand auch die Freiwilligkeit zur Zertifizierung im Vordergrund. Rechtlich bindende Regelwerke, wie z. B. Gesetze, sollten daher keine Rolle spielen. Bei den übrigen Regelwerken finden sich in der Praxis vor allem die Begriffe „Standards“, „Normen“ und „Frameworks“ wieder, welche im Alltag oftmals synonym verwendet werden. Jedoch dürfen nur offiziell ernannte Normungsorganisationen ihre Standards auch „Norm“ nennen.[9] Allein für den englischsprachigen Raum ist zu beachten, dass hier „Standard“ ein offizielles Regelwerk ernannter Organisationen bezeichnet und im Übrigen andere Begriffe verwendet werden. Im weiteren Verlauf dieser Arbeit wird die deutschsprachige Unterscheidung beibehalten, wenn von „Normen“ und „Standards“ im Fließtext geschrieben wird, unabhängig davon, ob eine Norm „Standard“ im Namen trägt oder nicht.

Ergebnisdokumente

Das aus einer Zertifizierung resultierende Ergebnisdokument, welches Dritten zugänglich gemacht werden soll, wird zwar oftmals als „Zertifikat“ bezeichnet, jedoch ist dies keine notwendige Konsequenz. Einerseits sehen einige Zertifizierungen andere Arten von Ergebnisdokumenten vor, wie im Weiteren dargestellt wird, andererseits wird der Begriff in anderen Zusammenhängen verwendet, welche die Definition verwässern. So erhalten etwa auch Personen nach der Teilnahme an Schulungsmaßnahmen Zertifikate, ohne dass eine Prüfung stattfand. In der Vernetzung von Computersystemen spielen sog. „digitale Zertifikate“ eine wichtige Rolle, da sie nach kryptographischen Verfahren bestimmte Eigenschaften von Personen oder Objekten bestätigen.[10] Und in der Finanzbranche wird mit „Zertifikat“ eine bestimmte Art von handelbaren Finanzprodukt beschrieben, welches Anteile an anderen Vermögenswerten darstellt.[11]

---

[8] Vgl. Klotz, 2012, S.10 ff.
[9] Art. 2 EU-Verordnung Nr. 1025/2012 - Eine interessante Ausnahme bildet hier die englischsprachige Variante dieser Verordnung, da sie an ebendieser Stelle das Wort „Standard“ benutzt, obwohl auch in anderen Sprachversionen, wie beispielsweise im Französischen oder Portugiesischen ebenfalls an dieser Stelle von „norme“ oder „norma“ gesprochen wird.
[10] Vgl. Porath, 2020, S. 356.
[11] Vgl. Larcher, 2020, S. 68 f.

3. Methodik der Auswahl

Einschränkungen der Auswahl

Im Rahmen dieser Arbeit werden nur freiwillige Zertifizierungen betrachtet, die unabhängig von der eigentlichen Geschäftsbeziehung durchgeführt werden können und die einen direkten oder indirekten Bezug zu Cloud-Services aufweisen.

Sammlung

Dazu wurden zuerst Zertifizierungen gesammelt, die bereits in der Literatur und Forschung Erwähnung fanden.[12] Weiterhin wurde überprüft, welche Zertifizierungen die drei Marktführer von Cloud-Services anbieten. Zum Zeitpunkt der Arbeit waren die Marktführer für Cloud-Services Microsoft mit 11,7% Anteil am weltweiten Markt für Cloud-Services, Amazon mit 10,8% sowie IBM mit 9,9%.[13] Zum Zeitpunkt der Studie gab Microsoft für dessen Cloud-Services Konformität zu insgesamt 92 Regelwerken,[14] Amazon zu 74 Regelwerken[15] und IBM zu 42 Regelwerken an.[16]

Verfeinerung

In die Vorauswahl wurden nur tatsächliche, von externen Dritten ausgestellte Zertifizierungen aufgenommen und auch nur solche, die Cloud-Service-Kunden freiwillig – also aus rein wirtschaftlichen Überlegungen und nicht wegen staatlicher Vorgaben – erwerben können. Zu letzteren würden beispielsweise Nachweise bezüglich der Einhaltung von Export- oder Importregularien gehören. Zum Schluss wurde mithilfe einer Expertengruppe aus dem IT-Governance-Bereich die Liste aufgrund ihrer Erfahrungen priorisiert. Dabei lag der Fokus vor allem darauf, die Relevanz der Zertifizierungen im DACH-Kontext zu betrachten. Die Liste hat dadurch zwar eine subjektive Einfärbung der Befragten bekommen, doch so wurde sie für das weitere Vorgehen reduziert.

Ergebnis

In der Folge umfasst die Vorauswahl Zertifizierungen, die…

- … auf einem vorab festgelegten Verfahren basieren, nach dem eine von den Geschäften des zu zertifizierenden Unternehmens unabhängige Instanz vorgegebene Anforderungen prüft und die Ergebnisse in einem Ergebnisdokument zusammenfasst, welches Dritten zur Verfügung gestellt werden kann;

[12] Vgl. Angaben aus Schneider & Sunyaev, 2015, S. 15 ff.; European Union Agency For Network And Information Security (ENISA), 2015, S. 31 ff.; Lins, 2019, S. 21 ff.
[13] https://www.itcandor.com/cloud-q219/ zuletzt abgerufen am 24.10.2020.
[14] Vgl. Microsoft 2021.
[15] Vgl. Amazon 2021.
[16] Vgl. IBM 2021.

- … Managementsysteme und Produkte auszeichnen;
- … auf freiwilliger Basis erworben werden und nicht zur Einhaltung gesetzlicher Normen zwingend erforderlich sind;
- … eine bereits vermutete Relevanz aufgrund der beschriebenen Auswahlkriterien innehaben.

Die dadurch ausgewählten Zertifizierungen wurden anhand des hauptsächlichen Nachweises als Ergebnisdokument in folgende Gruppierungen unterteilt:

- Zertifizierungen, die ein einseitiges Ergebnisdokument vorsehen;
- Zertifizierungen, die ein mehrseitiges Ergebnisdokument vorsehen;
- Zertifizierungen, die als Ergebnis hauptsächlich die Aufnahme in eine Liste vorsehen.

Einige der Zertifizierungen sehen mehrere Ergebnisdokumente vor, sodass sie potenziell auch anders eingruppiert werden könnten.

4. Ausgewählte Zertifizierungen

4.1 Zertifizierung mit einseitigem Ergebnisdokument

Einleitung

In der Praxis wird im Rahmen von Zertifizierungen am häufigsten der Begriff „Zertifikat“ für solche Ergebnisdokumente verwendet, die sich auf ein Logo, Gütesiegel oder eine einseitige Beschreibung reduzieren und die von den zertifizierten Unternehmen weitgehend frei genutzt werden.

4.1.1 Normen

Ergebnisdokument bei Normen

Das Nachweisdokument von Normen besteht nur aus zwei inhaltlichen Vorgaben:[17] Zum einen müssen Angaben zum zertifizierten Unternehmen (Name und geographischer Ort) zum anderen Randdaten des Zertifizierungsdokuments (Erteilungsdatum, Erweiterung oder Einschränkung des Geltungsbereichs) angegeben werden. Dies führt in der Regel dazu, dass das Ergebnisdokument zumeist nur eine Seite umfasst.

Zur Erlangung der Zertifizierung muss ein Audit durch eine akkreditierte

[17] Nach ISO/IEC 17021-1, Kap. 8.2.

Zertifizierungsstelle durchgeführt werden.[18] Die Zertifizierungsstelle wiederum muss durch die offizielle Akkreditierungsstelle des Landes akkreditiert sein. Die Gültigkeit der Zertifizierungen beträgt in der Regel drei Jahre. Innerhalb der drei Jahre müssen jährliche Überwachungsaudits durchgeführt werden.[19]

Zum aktuellen Zeitpunkt liegen zwölf harmonisierte und zertifizierbare internationale Normen vor.[20] Nach den beschriebenen Kriterien wurden die folgenden Normen ausgewählt.

(1) ISO/IEC 27001

Funktionsweise ISO/IEC-27001-Familie

Die ISO/IEC 27000-Familie wurde gemeinsam von der ISO und IEC entwickelt und veröffentlicht, um einen weltweit anerkannten Rahmen für Best Practices bezüglich Informationssicherheit zu schaffen. Die einzelnen Normen setzen dabei Schwerpunkte, unterstützen und ergänzen sich aber gegenseitig.

Umfang der ISO/IEC-27001

Die Norm „ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements“, vgl.Tabelle 1, enthält Anforderungen zur Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufenden Verbesserung eines dokumentierten Informationssicherheitssystems. Diese Norm soll für alle Organisationsarten und -größen anwendbar sein und stellt daher die Berücksichtigung der anwendenden Organisation auch besonders heraus.[21] Zu betonen ist, dass mit einer Zertifizierung nach ISO/IEC 27001 lediglich das Managementsystem zur Informationssicherheit zertifiziert wird, nicht der Grad der Informationssicherheit selbst. Um eine Zertifizierung zu erhalten, muss die Organisation bestimmte Kriterien zum Aufbau und zum Ablauf des Informationssicherheitsmanagementsystems nachweisen. Dazu gehören eine Risikoanalyse bezüglich der Sicherheit der zu betrachtenden Themen, den darin enthaltenen zu schützenden Informationen und den daraus entstehenden Risiken sowie die Ableitung relevanter Gegenmaßnahmen. Im Anhang der Norm, dem Annex A, befinden sich allgemeine Themen sowie vorgeschlagene Maßnahmen, die aufgrund ihrer Allgemeinheit im Rahmen des Risikomanagements berücksich-

[18] Vgl. DIN EN ISO 19011:2011, Kap. 7.1.
[19] Vgl. ISO/IEC 17021-1 Kap. 9.1.1
[20] Vgl. ISO, ISO Survey 2020.
[21] Vgl. ISO/IEC 27001, Kap. 1.

tigt werden müssen.[22] Dieser Annex A basiert wiederum auf der Norm „ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls“, die Best Practices und Erfahrungen zum allgemeinen Informationssicherheitsmanagementsystem darstellt.[23]

Tab. 1 Kerndaten zur ISO/IEC 27001

Titel	ISO/IEC 27001 IT-Sicherheitsverfahren – Informations-sicherheits-Managementsysteme – Anforderungen
Herausgeber	International Standards Organization
Typ	Norm
Aktuelle Version	06.2017
Gegenstand der Zertifizierung	Ein Managementsystem liegt vor, welches die Sicherheit von Informationen gewährleisten kann.
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	3 Jahre
Ergebnisdokument	Zertifizierungsdokument nach ISO/IEC 170021-1

Einbindung anderer Themen

Die Zertifizierungen anderer Standards der ISO 27000-Familie verlaufen ähnlich: Die ISO/IEC 27001 als Grundlage der Zertifizierung stellt Anforderungen an den Aufbau des zugrundeliegenden Managementsystems, während die weiteren Standards neue Themen, Risiken und Vorschläge zu Gegenmaßnahmen einbringen. Die Zertifizierung enthält dann jeweils einen entsprechenden Verweis auf die zusätzlich berücksichtigte Norm.

(2) ISO 9001

Umfang ISO 9001

Die Norm „ISO 9001 Quality management systems — Requirements“, vgl. Tabelle 2, legt für jede Organisation, unabhängig von Typ oder Größe oder den von ihr angebotenen Produkten und Dienstleistungen Anforderungen an ein Qualitätsmanagementsystem fest. Die Organisation muss dafür insbesondere nachweisen, dass sie in der Lage ist, ihre Leistung entsprechend der externen Anforderungen zu erbringen und stets an der Steigerung der Kundenzufriedenheit durch effektive Anwendung des Qualitätsmanagementsystems zu arbeiten.[24]

[22] Vgl. ISO/IEC 27001, Kap. 6.1.1.
[23] Vgl. ISO/IEC 27001, Kap. 6.1.3.
[24] Vgl. ISO 9001, Kap. 4.2.

Inhaltlich ist die ISO 9001 unspezifisch. Sie legt zwar fest, was umzusetzen ist, aber nicht, wie Prozesse und Arbeitsschritte im Detail ausgestaltet sein müssen. Dabei basiert sie auf vier Grundprinzipien, die das Handeln eines Unternehmens leiten sollen:

- **Kontext der Organisation**: Die Organisation muss interne wie externe Themen überwachen und überprüfen, welche für ihren Zweck und ihre strategische Ausrichtung von Bedeutung sind.[25]
- **Prozessorientierung**: Es sollte das Grundverständnis vorliegen, dass ein Unternehmen ein Zusammenwirken von ineinandergreifenden Prozessen ist.[26]
- **Risikomanagement**: In allen Phasen des Managementsystems sowie der Prozessdurchführung müssen Risiken und Chancen stets berücksichtigt werden. [27]
- **Fortlaufende Verbesserung**: Durch wiederholte Erhebung und Analyse der Prozessschritte und deren Ergebnisse soll eine kontinuierliche Verbesserung aller betrieblicher Vorgänge stattfinden. [28]

Die Zertifizierung belegt, dass das zertifizierte Unternehmen diese vier Prinzipien angemessen und wirksam umsetzt.

Tab. 2
Kerndaten zu ISO 9001

Titel	ISO 9001Qualitätsmanagementsysteme – Anforderungen
Herausgeber	International Standards Organization
Typ	Norm
Aktuelle Version	11.2017
Gegenstand der Zertifizierung	Ein Managementsystem liegt vor, welches die Qualität der Ergebnisse von Prozessen gewährleisten kann.
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	3 Jahre
Ergebnisdokument	Zertifizierungsdokument nach ISO/IEC 170021-1

[25] Vgl. ISO 9001, Kap. 4.1.
[26] Vgl. ISO 9001, Kap. 4.4.
[27] Vgl. ISO 9001, Kap. 6.1.
[28] Vgl. ISO 9001, Kap. 10.1.

(3) ISO/IEC 20000-1

Umfang ISO 20000

Der Standard „ISO/IEC 20000-1: Information technology — Service management — Part 1: Service management system requirements“, vgl. Tabelle 3, legt die Anforderungen fest, die eine Organisation einhalten sollte, um ein wirksames IT-Service-Managementsystem (ITSMS) einzurichten, zu implementieren, zu warten und kontinuierlich zu verbessern.[29] Im Mittelpunkt steht dabei vor allem die Erbringung der IT-Services im Sinne der externen Anforderungen durch eine integrierte prozessorientierte Vorgehensweise. Neben allgemeinen Anforderungen zur Aufbau- und Ablauforganisation identifiziert die Norm Anforderungen für Prozesse zum Service Design, Service Delivery, zum Beziehungsmanagement, zur Auflösung von Konflikten sowie zur Steuerung der Service-Bestandteile.[30]

Auch zur ISO/IEC 20000-1 gibt es ergänzende Normen, welche das reine ITSMS um spezifische Themen ergänzen. Für Cloud-Service-Anbieter beinhaltet der technische Report ISO/IEC TR 20000-9:2015 weitere Anforderungen.

Tab. 3
Kerndaten zu ISO/IEC 20000

Titel	ISO/IEC 20000-1 Informationstechnik - Service Management - Teil 1: Spezifikation für Service Management
Herausgeber	International Standards Organization
Typ	Norm
Aktuelle Version	04.2011
Gegenstand der Zertifizierung	Ein Managementsystem liegt vor, welches die Erbringung von IT-Services gewährleisten kann.
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	3 Jahre
Ergebnisdokument	Zertifizierungsdokument nach ISO/IEC 170021-1

(4) ISO 22301

Umfang ISO 22301

Der Fokus der „ISO 22301 Security and resilience – Business continuity management systems“, vgl. Tabelle 4, liegt vor allem auf Geschäftskontinuität und Notfallvorsorge. In diesem Dokument werden Anforderungen zur

[29] Vgl. ISO/IEC 20000-1, Kap. 1.
[30] Vgl. ISO/IEC 20000-1, Kap. 3.

Implementierung, Wartung und Verbesserung eines Managementsystems zur Vorbereitung auf Störungen festgelegt. Dadurch soll die anwendende Organisation geschäftsgefährdende Störungen erkennen, die Wahrscheinlichkeit des Auftretens dieser Störungen mindern, angemessene Reaktionen bei Eintritt vorbereiten und den Betrieb nach Abwendung wiederherstellen können. Dabei sind die Anforderungen allgemein gehalten und sollen für alle Organisationen, unabhängig von Typ, Größe und Art der Organisation gelten.[31]

Ausgangspunkt bildet demnach das Verständnis der Organisation und ihres Kontextes. Auf Basis einer sogenannten „Business Impact Analyse“ hat das Unternehmen festzulegen, welche Unterbrechungen es behandelt und welche Maßnahmen es zur Überwachung, Erkennung, Alarmierung, Kommunikation und Reaktion ergreift. Diese Maßnahmen müssen dann auch regelmäßig getestet und gegebenenfalls verbessert werden.

Tab. 4 Kerndaten zu ISO 22301

Titel	ISO 22301 - Sicherheit und Resilienz - Business Continuity Management System - Anforderungen
Herausgeber	International Standards Organization
Typ	Norm
Aktuelle Version	10.2019
Gegenstand der Zertifizierung	Ein Managementsystem liegt vor, welches einen möglichst unterbrechungsfreien Betrieb gewährleisten kann.
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	3 Jahre
Ergebnisdokument	Zertifizierungsdokument nach ISO/IEC 170021-1

4.1.2 Standards

Einführung

Neben den gesetzlich geregelten Normen gibt es Standards und Frameworks, die lediglich vereinfachte Ergebnisdokumente vorsehen. Dabei gilt es, sowohl Standards von öffentlichen Institutionen als auch von privaten Organisationen zu berücksichtigen.

[31] Vgl. ISO 22301, Kap. 1.

(1) IT-Grundschutz

Öffentliche Aufgaben

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach § 3 Abs. 1 BSI-Gesetz (BSIG) die Aufgabe, die Sicherheit in der Informationstechnik zu fördern. Dazu gehört unter anderem auch die Zertifizierung informationstechnischer Systeme nach § 9 des BSIG.

Grundlage der Zertifizierung

Das BSI hat als sogenanntes „IT-Grundschutz-Kompendium“ Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen in Bezug auf Informationssicherheit zusammengestellt, die die Grundlage für die Zertifizierung „ISO 27001 Zertifizierung auf Basis von IT-Grundschutz“ bilden, vgl. Tabelle 5.[32]

Ablauf der Zertifizierung

Die Zertifizierung verläuft ähnlich wie bei der ISO/IEC 27000 Familie. Der mit dem ISO/IEC 27001 kompatible BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit. Das IT-Grundschutz-Kompendium enthält die IT-Grundschutz-Bausteine, in denen jeweils anhand der BSI-Standards 200-2 und 200-3 Gefährdungen und Sicherheitsanforderungen zu einzelnen Themen adressiert werden. Ein vom BSI zertifizierter ISO 27001-Grundschutz-Auditor führt daraufhin die Prüfung durch und erstellt einen Auditbericht. Dieser Auditbericht muss dem BSI zur Prüfung vorgelegt werden, das dann über die Ausstellung der Zertifizierung entscheidet.[33]

Tab. 5 Kerndaten zu IT-Grundschutz

Titel	ISO 27001 Zertifizierung auf Basis von IT-Grundschutz
Herausgeber	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Typ	Standard
Aktuelle Version	Version 4.3 vom 01.02.2020
Gegenstand der Zertifizierung	Ein Managementsystem liegt vor, welches die Sicherheit von Informationen gewährleisten kann und dabei die Vorgaben des BSI beachtet
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	3 Jahre
Ergebnisdokument	Zertifizierungsdokument nach ISO 170021, ergänzt um den Zusatz „auf Basis des IT-Grundschutzes“

[32] Vgl. BSI, 2019 S. 8.
[33] Vgl. BSI, 2019 S. 8 ff.

(2) EuroCloud Star Audit (EuroCloud-SA)

Herausgeber

EuroCloud® Europe a.s.b.l. (EuroCloud) ist eine internationale Non-Profit-Organisation, welche die Aktivitäten verschiedener Personen und Organisationen im europäischen Raum vereint, um Aufbau und Weiterentwicklung europäischer Cloud-Lösungen voranzutreiben. Zur Förderung des Vertrauens in die Cloud-Wirtschaft wurde die StarAudit-Initiative geschaffen.[34]

Vorgehen

Der Kriterienkatalog von StarAudit, vgl. Tabelle 6, umfasst mehrere Faktoren, die Cloud-Services als Dienstleistung ausmachen. Dazu gehören neben der Bewertung technischer Sicherheits- und Rechtsfragen eine Service-spezifische Beurteilung sowie weitere Aspekte, wie die Lieferkette.[35] Der Cloud-Service-Anbieter kann anhand eines Fragebogens auf der Webseite von StarAudit seinen eigenen Vorbereitungsstand prüfen und einreichen. Daraufhin werden diese Angaben durch akkreditierte Auditoren überprüft. Sofern alle Anforderungen erfüllt sind, wird nach eingereichtem Bericht der Auditoren ein „Zertifikat“ genanntes PDF-Dokument ausgestellt und der Name des Cloud-Service-Anbieters wird in der offiziellen Liste geführt. [36]

Tab. 6 Kerndaten zu EuroCloud Star Audit

Titel	StarAudit
Herausgeber	EuroCloud® Europe a.s.b.l.
Typ	Standard
Aktuelle Version	Version 4.0 Rev. 04 vom 15.12.2020
Gegenstand der Zertifizierung	Bereitstellung von Cloud-Services
Cloud-Bezug	direkt
Zeitliche Aussagekraft	2 Jahre
Ergebnisdokument	Einseitiges PDF und Listung auf https://staraudit.org/de/all-certificates/

4.2 Zertifizierung mit mehrseitigem Ergebnisdokument

Einleitung

Einseitige Ergebnisdokumente können einen Konformitätsstatus lediglich binär angeben. Da es in den meisten Fällen aber Lücken bei der Konformität

[34] Vgl. EuroCloud, S. 4.
[35] Vgl. EuroCloud, S. 12.
[36] Vgl. EuroCloud, https://staraudit.org/de/all-certificates/, zuletzt abgerufen am 28.12.2020.

mit allen Anforderungen des zugrundeliegenden Regelwerkes gibt, wäre dies eine verkürzte Darstellung. Einige Zertifizierungen sehen daher ausführlichere Darstellungen als Ergebnisdokumente vor.

4.2.1 Berichte von Wirtschaftsprüfungsgesellschaften

Herleitung

Ein häufiger Typus von Zertifizierungen sind Berichte von Wirtschaftsprüfungsgesellschaften als Nachweis zur Einhaltung von Vorgaben. Aufgabe der Wirtschaftsprüfer ist es, betriebswirtschaftliche Prüfungen, insbesondere bezüglich der Jahresabschlüsse, durchzuführen und Berichte über die Ergebnisse solcher Prüfungen auszustellen.[37] Diese ursprünglich lediglich auf die ordentliche Buchführung bezogene Aufgabe wurde im Laufe der Jahre um immer weitere Fragestellungen erweitert. Für bestimmte Themen wurden daher sogenannte „Prüfungsstandards“ erstellt, welche zu bestimmten prüferischen Fragestellungen und Themen Vorgaben enthalten und somit bei der Durchführung von Prüfungen grundsätzlich zu beachten sind.

(1) IDW PS 951 / ISAE 3402

Gegenstand der Prüfung

Gegenstand des Prüfungsstandards 951 des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW PS 951) sowie seines internationalen Pendants, dem International Standard on Assurance Engagements 3402 (ISAE 3402) der American Institute of Certified Public Accountants, sind interne Kontrollsysteme (IKS) von Dienstleistungsunternehmen.[38]

Das Unternehmensmanagement hat aufgrund verschiedener Vorgaben[39] die Aufgabe, unternehmerische Risiken, die aus dem Einsatz von IT entstehen, durch angemessene Regelungen zu steuern. Das interne Kontrollsystem stellt die Gesamtheit dieser aufbau- und ablauforganisatorischen Regelungen dar.[40] Die Standards IDW PS 951, vgl. Tabelle 7, und das internationale Pendant ISAE 3402, vgl. Tabelle 8, stellen Vorgaben auf, wie Kontrollen eines Unternehmens mit Bezug zu dessen Dienstleistung geprüft werden. Im Ergebnis wird ein Bericht darüber erstellt, anhand dem Kunden nachvollziehen können, welche Kontrollmaßnahmen die Qualität der Dienstleistung gewährleisten und welche Sachverhalte und Nachweise dazu von den Prüfern betrachtet wurden.

---

[37] § 2 WPO; Vgl. IDW, 2015, Tz. 1; IFAC, 2009, Tz. 3.
[38] Vgl. IDW, 2013, IFA 2011.
[39] Bspw. für Aktiengesellschaften die Pflicht zur Einrichtung eines Risikofrüherkennungssystems nach § 91 Abs. 2 AktG.
[40] Vgl. Kersten, et al., 2020, S. 245.

Titel	IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen (IDW PS 951)
Herausgeber	Institut der Wirtschaftsprüfer in Deutschland e. V
Typ	Standard
Aktuelle Version	16.10.2013
Gegenstand der Zertifizierung	Nachvollziehbares wirksames und angemessenes dienstleistungsbezogenes internes Kontrollsystem
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	Vorausgehende 12 Monate, jährliche Überprüfung notwendig
Ergebnisdokument	Mehrseitiger Bericht

Tab. 7
Kerndaten zum IDW PS 951

Berichtsarten

Dabei wird auf zwei Arten geprüft: Beim sogenannten Typ 1-Bericht wird zunächst die Angemessenheit der implementierten Maßnahmen in Bezug auf die verfolgten Ziele betrachtet und bewertet. Für einen Typ 2-Bericht werden neben der Angemessenheit auch die tatsächliche Implementierung der Kontrollmaßnahmen für einen definierten Zeitraum sowie deren Wirksamkeit mittels statistisch aussagekräftiger Stichproben durch die Wirtschaftsprüfer geprüft.[41]

Titel	International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a service Organization
Herausgeber	International Federation of Accountants
Typ	Standard
Aktuelle Version	15.06.2011
Gegenstand der Zertifizierung	Nachvollziehbares wirksames und angemessenes dienstleistungsbezogenes internes Kontrollsystem
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	Vorausgehende 12 Monate, jährliche Überprüfung notwendig
Ergebnisdokument	Mehrseitiger Bericht

Tab. 8
Kerndaten zu ISAE 3402

[41] Vgl. IDW, 2013.

Mehrwert

Cloud-Service-Kunden haben durch diesen Bericht die Möglichkeit, die vom Cloud-Service-Anbieter selbst identifizierten und ergriffenen Maßnahmen und zugrundeliegenden Standards, die qualitativen Prüfungen sowie die zusammengefassten Ergebnisse der Wirtschaftsprüfer einzusehen.

(2) Anforderungskatalog C5 des BSI

Umfang

Speziell für Cloud Computing hat das BSI den „Cloud Computing Compliance Criteria Catalogue“ (C5), vgl. Tabelle 9, erarbeitet. Dieser spezifiziert explizit Anforderungen an sicheres Cloud-Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter sowie deren Prüfer und Kunden.[42]

Tab. 9
Kerndaten zum C5

Titel	Cloud Computing Compliance Criteria Catalogue
Herausgeber	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Typ	Standard
Aktuelle Version	19.01.2020
Gegenstand der Zertifizierung	Nachvollziehbares wirksames und angemessenes dienstleistungsbezogenes internes Kontrollsystem von Cloud Service Anbietern
Cloud-Bezug	direkt
Zeitliche Aussagekraft	Vorausgehende 12 Monate, jährliche Überprüfung notwendig
Ergebnisdokument	Mehrseitiger Bericht nach IDW PS 951 oder ISAE 3402

Prüfung nach ISAE 3402 / IDW PS 951

Bei Erarbeitung hat sich das BSI an nationalen und internationalen Normen orientiert. Daher sollen zur Durchführung der Prüfung sowie zur Erstellung des zertifizierenden Berichtes die Vorgaben aus ISAE 3402 bzw. IDW PS 951 zugrunde gelegt werden.[43]

(3) System and Organization Controls (SOC)

Beschreibung

Die vom American Institute of Certified Public Accountants (AICPA) veröffentlichten System- und Organisationskontrollen (SOC), vgl. Tabelle 10, wurden für Organisationen definiert, die Informationssysteme als Service bereitstellen. Anhand der SOC sollen validierte Berichte über vorhandene

[42] Vgl. BSI, 2020, S. 15.
[43] Vgl. BSI, 2020, S. 18.

Kontrollmaßnahmen für Nutzer dieser Informationssysteme bereitgestellt werden.[44] Die Berichte werden anhand von festgelegten Kontrollen erstellt, die in fünf Kategorien unterteilt sind und als Trust Service Principles (TSC) bezeichnet werden.

Berichtsarten

Bei den Berichten wird zwischen drei Arten unterschieden:[45]

- **SOC 1 — Interne Kontrollen über die Finanzberichterstattung**: Hier werden, wie bei IDW PS 951 und ISAE 3402 auch, die Angemessenheit und Wirksamkeit der vom Unternehmen definierten Kontrollen geprüft, wobei die TSC lediglich einen Maßstab für die Bewertung dieser darstellen.
- **SOC 2 — Trust Services Criteria:** Beim SOC 2-Bericht hingegen wird die angemessene Verwendung der TSC in den Kontrollen geprüft. Wichtiger ist hier, dass alle relevanten TSC wirksam und angemessen angewendet wurden, sich also in Kontrollen wiederfinden.
- **SOC 3 — Trust Services Criteria for General Use Report:** Bei SOC 3-Berichten handelt es sich um verkürzte Berichte zur Anwendung der TSC für Service-Nutzer, die Sicherheit in Bezug auf die TSC benötigen, jedoch einen SOC 2-Bericht nicht effektiv nutzen könnten.

Prüfung

Die Berichte werden anhand der Vorgaben des Statements on Standards for Attestation Engagements (SSAE) No. 18 erstellt, welcher wiederum den ISAE 3402 entspricht.[46]

Tab. 10
Kerndaten zu SOC

Titel	System and Organization Controls (SOC) anhand der Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
Herausgeber	American Institute of Certified Public Accountants (AICPA)
Typ	Standard
Aktuelle Version	März 2020
Gegenstand der Zertifizierung	Nachvollziehbares wirksames und angemessenes dienstleistungsbezogenes internes Kontrollsystem von Anbietern von Informationsdiensten

[44] Vgl. AICPA 2020 S. 2.
[45] Vgl. AICPA 2018 S. 4.
[46] Vgl. AICPA,2016a zur Verknüpfung von ISAE 3402 und SSAE 16, wobei SSAE 16 bereits von SSAE 18 ersetzt wurde, s. AICPA 2016b.

Cloud-Bezug	indirekt
Zeitliche Aussagekraft	Vorausgehende 12 Monate, jährliche Überprüfung notwendig
Ergebnisdokument	Mehrseitiger Bericht nach ISAE 3402

4.2.2 Andere mehrseitige Ergebnisdokumente

Als Standards mit mehrseitigen Ergebnisdokumenten wurden „NIST CSF“ und „PCI DSS“ betrachtet.

(1) NIST CSF

Beschreibung

Das Cyber Security Framework (CSF) ist ein vom National Institute of Standards and Technology (NIST) erarbeitetes, freiwillig anwendbares Referenzwerk zum Management der Informationssicherheit nach Best-Practice-Ansätzen, vgl. Tabelle 11.[47] Dabei werden mithilfe von 98 Zielvorgaben Anforderungen an vorgefertigte Profile gestellt. Jedoch wird nicht vorgegeben, wie diese zu erreichen seien.

Rückgriff auf andere Prüfungen

Das NIST selbst bietet auch keine Zertifizierungen für den Standard an. Die Einhaltung dieses Standards kann aber durch die Einhaltung anderer Standards nachgewiesen werden, die nach dem sog. OLIR-Programm entsprechend akkreditiert sind.[48]

Beispiel HITRUST CSF

Ein Beispiel hierfür ist das HITRUST CSF der Health Information Trust Alliance (HITRUST). Dieses liefert Anwendungshinweise, die zur Umsetzung jedes der Cybersicherheitsziele des NIST CSF erforderlich sind, ergänzt diese aber noch um einige relevante Aspekte aus dem Healthcare-Bereich. Der HITRUST CSF unterstützt die Berichterstattung bezüglich des NIST CSF mithilfe einer sogenannten „NIST CSF Scorecard“ die in jedem validierten HITRUST CSF-Bewertungsbericht enthalten ist. Sie gibt an, wie gut eine Organisation, die in den NIST CSF-Kernunterkategorien festgelegten Ziele erreicht, basierend darauf, wie gut sie die zugrunde liegenden HITRUST CSF-Kontrollen implementiert hat.[49]

[47] Vgl. NIST, 2018, S. 6.
[48] Vgl. NIST, 2020. S.2.
[49] Vgl. HITRUST 2020.

Titel	NIST Cybersecurity Framework
Herausgeber	National Institute of Standards and Technology (NIST)
Typ	Framework
Aktuelle Version	Version 1.1, April 2018
Gegenstand der Zertifizierung	Fähigkeitsgrad zur Verhinderung, Erkennung und Reaktion auf Cyberangriffe
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	Zurückliegendes Jahr
Ergebnisdokument	Bericht

Tab. 11
Kerndaten zu NIST CSF

(2) PCI DSS

Beschreibung

Der Payment Card Industry Data Security Standard (PCI DSS), vgl. Tabelle 12, ist ein Sicherheitsstandard zum Schutz von Kreditkartendaten. Dabei handelt es sich um technische und betriebliche Anforderungen, die vom PCI Security Standards Council (PCI SSC) zum Schutz von Karteninhaberdaten festgelegt wurden. Die Standards gelten für alle Organisationen, die Karteninhaberdaten speichern, verarbeiten oder übertragen. Unternehmen müssen sich nicht aufgrund gesetzlicher Pflichten an diesen Standard halten. Aber bei Nichteinhaltung wird die Verarbeitung von Kreditkartendaten durch die Gründungsmitglieder des PCI SSC, American Express, Discover Financial Services, JCB International, MasterCard Worldwide und Visa Inc. verwehrt oder vertraglich durchgesetzt.[50]

Vorgehen

Kernpunkt des Standards sind Anforderungen an die Einrichtung der Rechnernetze von Unternehmen. Über individuelle Berichte wird der jeweilige PCI DSS-Konformitätsstatus dargestellt. Abhängig von den Anforderungen der Zahlungskartenmarke sowie der Anzahl der Transaktionsdaten müssen die anwendenden Unternehmen entsprechende Selbstbewertungsfragebögen (SAQ)[51] ausfüllen. Diese müssen von einer von der PCI SSC akkreditierten Organisation bestätigt werden. Gegebenenfalls ist die vierteljährliche Einreichung eines Berichts über die Ergebnisse eines Scans der Netzwerkeinstellungen erforderlich.[52]

[50] Vgl. PCI Security Standards Council, 2009, S. 6.
[51] Vgl. PCI Security Standards Council, 2018.
[52] Vgl. PCI Security Standards Council, 2009, S. 35.

Titel	Payment Card Industry (PCI) Data Security Standard
Herausgeber	PCI Security Standards Council
Typ	Standard
Aktuelle Version	01.05.2018
Gegenstand der Zertifizierung	Netzwerk-Konfiguration gemäß den Vorgaben des Standards
Cloud-Bezug	Indirekt
Zeitliche Aussagekraft	2 Jahre
Ergebnisdokument	Bestätigte Selbstauskünfte

Tab. 12 Kerndaten zu PCI DSS

4.3 Zertifizierung durch Auflistung

Aufnahme in Listen

Der für die Cloud-Service-Kunden einsehbare Nachweis zur Konformität besteht für die Zertifizierungen dieses Abschnitts in der Aufnahme des Firmennamens des Unternehmens oder dessen Produkt in im Internet öffentlich einsehbare Listen. Hier muss die Definition der Zertifizierung etwas weiter verstanden werden, da nicht zwangsläufig einzelne Dokumente ausgestellt werden, die der Cloud-Service-Anbieter seinen Kunden bereitstellen kann. Dies ist zumindest nicht das primäre Ziel. Zwar werden in solchen Fällen auch Berichte und Ergebnisse dokumentiert, dennoch soll hauptsächlich die Aufnahme des Firmennamens in die Auflistungen, die die Kunden einsehen können, das Einhalten der zugrundeliegenden Anforderungen darstellen.

Vorteil

Ein Vorteil in dieser Vorgehensweise besteht aus Sicht der Zertifizierungsstellen darin, dass sie selbst besser kontrollieren können, von welchen Unternehmen sie referenziert werden. Die Fälschung von Ergebnisdokumenten ist technisch nicht schwer, was bei Missbrauch auch die Integrität der Zertifizierungsstellen in Frage stellt. Durch Einsicht in ausschließlich durch die Zertifizierungsstellen verwaltete Listen können die Kunden den Sachverhalt unabhängig vom Cloud-Service-Anbieter nachvollziehen.

Betrachtungsumfang

Einige Zertifizierungsstellen bieten beide Varianten an, also die Übergabe eines Dokuments neben der Aufnahme in eine entsprechende Liste. In diesem Abschnitt werden aber nur die Zertifizierungen dargestellt, die sich hauptsächlich durch die Auflistung der zertifizierten Objekte äußern.

(1) Trusted Cloud

Zielsetzung

Trusted Cloud, vgl. Tabelle 13, ist eine Initiative des Bundesministeriums für Wirtschaft und Energie (BMWi). Ziel dieser Initiative ist es, Vertrauen in Cloud Services durch einheitliche und transparente Bewertungskriterien aufzubauen.[53] Dafür wurde eigens der Trusted Cloud Kompetenznetzwerk e.V. ins Leben gerufen.

Erlangung

Cloud-Service-Anbieter müssen zur Listung angeben, inwiefern sie einem vorbereiteten Kriterienkatalog entsprechen. Dieser Kriterienkatalog legt den Fokus vor allem auf Transparenz der Dienstleistung und beleuchtet weniger bzw. indirekt andere Aspekte, wie Sicherheit oder Qualität.[54] Alle Angaben werden in einem Portal hochgeladen und durch einen externen Prüfer bestätigt. Das Ergebnis des Prüfers wird anschließend bei der Entscheidung des „Trusted Cloud-Beirats“ zur Listung berücksichtigt.[55]

Als Ergebnis werden Cloud-Service-Anbieter in der Listung aufgenommen und erhalten ein individuelles Trusted Cloud Label für Ihren Service. Die Dauer der Gültigkeit geht aus dem Vertrag zwischen der Plattform und dem Cloud-Service-Anbieter hervor, welche zuletzt bei 36 Monaten lag.[56]

Tab. 13
Kerndaten zu Trusted Cloud

Titel	Trusted Cloud
Herausgeber	Trusted Cloud Kompetenznetzwerk e.V
Typ	Standard
Aktuelle Version	Kriterienkatalog 2.0 vom 30.05.2018
Gegenstand der Zertifizierung	Transparenz und Vertrauenswürdigkeit der erbrachten Cloud Services
Cloud-Bezug	Direkt
Zeitliche Aussagekraft	Je nach Vertragsschluss (akt. 3 Jahre)
Ergebnisdokument	Listung und Logo

(2) CIS Benchmarks

Beschreibung

Das Center for Internet Security (CIS) ist eine gemeinnützige internationale

[53] Vgl. BMWi, 2021.
[54] Vgl. Trusted Cloud Kompetenznetzwerk e.V., 2018, S. 6.
[55] Vgl. Trusted Cloud Kompetenznetzwerk e.V., 2020.
[56] Vgl. Trusted Cloud Kompetenznetzwerk e.V., 2017, S. 11.

Organisation, welche sogenannte CIS Benchmarks, vgl. Tabelle 14, veröffentlicht und weiterentwickelt.[57] CIS-Benchmarks sind Best Practices zur sicheren Konfiguration und zum Umgang mit IT-Systemen, die zahlreiche weitere Normen und Standards berücksichtigen. Während in den meisten Standards und Normen meist nur sehr vage Andeutungen vorhanden sind, beschreiben die CIS-Benchmark-Dokumente konkrete Handlungsanweisungen und Befehl-Vorgaben zur Umsetzung und Überprüfung der Anforderungen. Entsprechend können damit nur konkrete Produkte, aber keine Managementsysteme auditiert werden.

Vorgehen

Durch die konkrete Konfigurationsvorgabe kann die Auditierung der Vorgaben automatisiert geschehen. Das zu zertifizierende Unternehmen muss zur Überprüfung lediglich die entsprechende Datei herunterladen.[58] Aus der Überprüfung entstehen kryptographische Prüfsummen, die das CIS nur noch gegenprüfen muss. War das Audit erfolgreich, werden Produkt und Hersteller auf der offiziellen Seite geführt. Zudem erhält der Hersteller ein Logo, das er zu Marketingzwecken verwenden darf.[59]

Tab. 14 Kerndaten zu CIS Benchmarks

Titel	CIS Benchmark (je auditierendes IT-System eigene Bezeichnung)
Herausgeber	Center for Internet Security (CIS)
Typ	Standard
Aktuelle Version	je auditierendes IT-System eigener Versionsstand
Gegenstand der Zertifizierung	Sichere Einstellung von IT-Systemen nach geprüften und bewährten Best Practices
Cloud-Bezug	Indirekt (Auditierung der zugrundeliegenden Technologien) direkt (ausgewählte Public-Cloud-Services)
Zeitliche Aussagekraft	Bis zur Veröffentlichung einer neuen Major-Version des geprüften CIS Benchmarks
Ergebnisdokument	Listung und Logo

(3) CSA STAR

CSA STAR

Das Cloud Security Alliance - Security Trust Assurance and Risk (CSA STAR) ist ein von der Cloud Security Alliance im Jahre 2012 eingeführtes

[57] Vgl. CIS, https://www.cisecurity.org/about-us/ zuletzt abgerufen am 24.10.2020.
[58] Vgl. CIS, https://www.cisecurity.org/cis-securesuite/pricing-and-categories/product-vendor/cis-benchmark-assessment/, zuletzt abgerufen am 24.10.2020.
[59] Vgl. CIS, https://www.cisecurity.org/cis-benchmarks/, zuletzt abgerufen am 24.10.2020.

Register zertifizierter Cloud-Service-Anbieter, vgl. Tabelle 15.[60] Anhand eines Fragebogens, in dem Cloud-spezifische Sicherheitskontrollen enthalten sind, können die Cloud-Service-Anbieter ihren Vorbereitungsstatus selbst prüfen.

Mehrere Level

Die Auflistung von Cloud-Service-Anbietern basiert auf drei Leveln der Einhaltung des STAR Frameworks.[61] Um in dem Register nach Level 1 aufgeführt zu werden, müssen Cloud-Service-Anbieter lediglich eine Selbsteinschätzung der Einhaltung einreichen. Level 2 hingegen beinhaltet bereits die Prüfung durch Drittparteien, wohingegen Level 3 einen dynamischen Zertifizierungsansatz verfolgt.[62] Ab Level 2 gibt es die Möglichkeit, sowohl einen ausführlichen Bericht („Attestation“) auf Grundlage des ISAE 3402 Reportings[63] oder ein Zertifikat („Certification“) auf Grundlage der Normen ISO/IEC 17021-1 oder DIN EN ISO 19011 zu erhalten.[64]

Tab. 15
Kerndaten zu CSA STAR

Titel	CSA Security Trust, Assurance and Risk (STAR)
Herausgeber	Cloud Security Alliance (CSA)
Typ	Standard
Aktuelle Version	2019
Gegenstand der Zertifizierung	Der betrachtete Cloud Service erfüllt die Anforderungen des CSA STAR
Cloud-Bezug	direkt
Zeitliche Aussagekraft	Level 1: Unbegrenzt Level 2: Bericht für zurückliegendes Jahr, Zertifikat für 3 Jahre Level 3: dauerhaft
Ergebnisdokument	Level 1: Listung Level 2: Bericht und/oder Zertifikat Level 3: Listung

(4) TISAX

Hintergrund

Das Trusted Information Security Assessment Exchange (TISAX), vgl. Tabelle 16, ist ein von der deutschen Automobilindustrie ins Leben gerufener Prüf- und Austauschmechanismus zur Sicherstellung der Informationssicher-

[60] Vgl. CSA, 2019, S. 3.
[61] Vgl. CSA, 2019, S. 5.
[62] S.o. Abschnitt 2.3.3.
[63] Vgl. CSA, 2019, S. 6.
[64] Vgl. CSA, 2019, S. 7.

heit. Er soll die Informationssicherheit vor allem im Automobilsektor sicherstellen und die gemeinsame Anerkennung von Prüfergebnissen zwischen den Teilnehmenden ermöglichen.[65] Als Grundlage für die Prüfungen gilt der Katalog zum Information Security Assessment des Verbands der Automobilindustrie (VDA ISA),[66] welcher verschiedene Stufen der Informationssicherheit festlegt. Unternehmen, die am TISAX teilnehmen wollen, müssen sich an einer zentralen Plattform anmelden und ein Prüfziel festlegen.[67] Es gibt insgesamt acht Prüfziele, anhand derer sich Tiefe und Aufwand der Prüfung orientieren.[68]

Vorgehen

Für das TISAX gibt es eigens zugelassene Prüfer, die die Konformität des VDA ISA beim Unternehmen prüfen dürfen.[69] Am Ende der Prüfung erstellt der Prüfdienstleister einen offiziellen TISAX-Bericht.[70] Dieser enthält auch ein zusammenfassendes TISAX-Label, welches die Prüfziele und das Prüfergebnis zusammenfassen.[71] Nachdem Unternehmen die Prüfung erfolgreich absolviert haben, wird der Bericht zusammen mit der geprüften Stufe im TISAX-Portal angezeigt.[72]

Tab. 16 Kerndaten zu TISAX

Titel	Trusted Information Security Assessment Exchange (TISAX)
Herausgeber	ENX Association
Typ	Standard
Aktuelle Version	2019
Gegenstand der Zertifizierung	Informationssicherheit wird gemäß des VDA ISA anhand der korrespondierenden Sicherheitseinstufung umgesetzt.
Cloud-Bezug	indirekt
Zeitliche Aussagekraft	3 Jahre
Ergebnisdokument	Listung

[65] S. ENX Association, https://portal.enx.com/de-DE/TISAX/, zuletzt abgerufen am 24.10.2020.
[66] S. VDA, https://www.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen.html, zuletzt abgerufen am 24.10.2020.
[67] Vgl. ENX Association, 2020, S. 13 f.
[68] Vgl. ENX Association, 2020, S. 33 ff.
[69] Vgl. ENX Association, 2020, S. 67.
[70] Vgl. ENX Association, 2020, S. 14.
[71] Vgl. ENX Association, 2020, S. 81.
[72] Vgl. ENX Association, 2020, S. 84 ff.

(5) FedRamP

Hintergrund

Das Federal Risk and Authorization Management-Programm (FedRAMP), vgl. Tabelle 17, ist ein Programm der Regierung der Vereinigten Staaten von Amerika, das einen standardisierten Ansatz für die Sicherheitsbewertung, Autorisierung und kontinuierliche Überwachung von Cloud-Produkten und Cloud-Diensten bietet.[73] Die Mission des FedRAMP besteht darin, die Einführung sicherer Cloud-Dienste in der gesamten US-Bunderegierung zu fördern, indem ein standardisierter Ansatz für die Sicherheits- und Risikobewertung bereitgestellt wird. Nichtsdestotrotz können diese Vorgaben auch im privaten Sektor angewendet werden. Grundlage für die Zertifizierung ist die von dem US-Institut NIST herausgegebene Special Publication (SP) 800-53. FedRAMP ist das Programm, das bescheinigt, dass ein Anbieter von Cloud-Diensten diese Standards erfüllt.

Vorgehen

Zunächst muss ein Cloud-Service-Anbieter einen Systemsicherheitsplan (SSP) anhand der NIST SP 800-53 erstellen, der die Sicherheitsvorlage seines Systems darstellt. Der SSP wird daraufhin von einer Assessment Organization (AO) auf Angemessenheit und Wirksamkeit geprüft.[74] Nach Abschluss erstellt die AO einen Security Assessment Report (SAR-Bericht), in dem die Ergebnisse detailliert beschrieben sind und eine Empfehlung für die FedRAMP-Autorisierung enthalten ist.[75] Behörden überprüfen dann die Bewertung und die damit verbundenen Ergebnisse und genehmigen sie entweder oder fordern zusätzliche Tests an. Wenn die Behörden das mit der Nutzung des Systems verbundene Risiko akzeptieren, und das Cloud-Service-Produkt des Cloud-Service-Anbieters bestätigen, werden beide einer zugangsbeschränkten Liste unter www.fedramp.gov hinzugefügt. Die Liste enthält grundlegende Informationen zum Serviceangebot für das autorisierte System.[76]

Kontinuierliche Überwachung

Sobald ein Cloud-Service-Anbieter zertifiziert ist, muss er eine kontinuierliche Überwachungsfunktion implementieren, um sicherzustellen, dass der Cloud-Service eine akzeptable Risikostellung beibehält. Dazu müssen jährliche Bewertungen durchgeführt werden und der FedRAMP-Organisation ein monatlicher Bericht vorgelegt werden.[77]

---

[73] Vgl. Fedramp Programm Management Office, 2017, S. 2.
[74] Vgl. Fedramp Programm Management Office, 2017, S. 11.
[75] Vgl. Fedramp Programm Management Office, 2017, S. 12.
[76] Vgl. Fedramp Programm Management Office, 2017, S. 17.
[77] Vgl. Fedramp Programm Management Office, 2017, S. 18.

Titel	Federal Risk and Authorization Management-Programm
Herausgeber	Konsortium mehrerer US-amerikanischer Behörden
Typ	Framework
Aktuelle Version	Version 2.4, 15.11.2017
Gegenstand der Zertifizierung	Systemsicherheitsplan des Cloud-Service-Anbieters erfüllt die Voraussetzungen der NIST SP 800-53 angemessen und wirksam.
Cloud-Bezug	Direkt, sowohl IaaS, PaaS als auch SaaS
Zeitliche Aussagekraft	Maximal 1 Jahr
Ergebnisdokument	Listung

Tab. 17 Kerndaten zu FedRAMP

(6) Andere Listen, die nicht in der Vorauswahl enthalten sind

Wissens-Zertifizierungen

Die Art des Nachweises zur Konformität von Anforderungen durch Dritte wird vor allem auch bei der sogenannten Partner-Zertifizierung von Herstellern gewählt. Dadurch wird dargestellt, dass die aufgelisteten Unternehmen angemessenes Wissen zum Umgang mit den Produkten des Herstellers haben.

US Privacy Shield

Insbesondere in Bezug auf Datenschutz sei hier erwähnt, dass diese Nachweisart auch bei der Zertifizierung von US-basierten Unternehmen zum Nachweis der Einhaltung der Vorgaben des europäischen Datenschutzes genutzt wird. Sowohl für das Projekt „Privacy Shield“ als auch das Vorgängermodell „Safe Harbour“ bestanden entsprechende Listen.[78]

5. Ergebnisse der zugrundeliegenden Studie

Hintergrundstudie

Diese Übersicht von Standards und Zertifizierungen wurde im Rahmen einer Abschlussarbeit für eine Studie zur Bewertung der Relevanz der Zertifizierungen aus Sicht von potenziellen Cloud Service-Kunden erstellt. Dazu wurde mit Hilfe einer Online-Umfrage sowie einigen Expertengesprächen ermittelt, welche dieser Zertifizierungen am ehesten dazu geeignet seien, das Vertrauen in Cloud-Services zu stärken und warum dies so sei. Die Ergebnisse lassen sich wie folgt zusammenfassen.

[78] Vgl. U.S. Department of Commerce 2021.

Fokus wichtiger als Bekanntheit

Der Fokus der Zertifizierung ist demnach als Faktor wichtiger als die eigentliche Bekanntheit der Zertifizierung. So wurden vor allem Zertifizierungen, die ein Sicherheitsniveau für Informationen attestieren, von den Teilnehmenden der Studie als relevanter angesehen als Zertifizierungen für Qualität, auch wenn deren zugrundeliegenden Standards eine vergleichbare Bekanntheit bei den Befragten erreichte.

Bevorzugt öffentlich geförderte

Tendenziell wurden Zertifizierungen als relevanter bewertet, wenn sie auf Regelwerken basieren, die öffentlich gefördert werden, wie etwa Normen oder Standards öffentlicher Stellen.

Marktindividuelle Anforderungen

Die Einzelgespräche zeigten auf, dass im Einzelfall die Relevanzbewertung aber auch stark von den externen Anforderungen an das Projekt abhängig sein kann. Vor allem sei dies der Fall, wenn Zertifizierungen direkte oder indirekte Pflichtvorgabe für das jeweilige Geschäftsfeld des Kunden darstellen, wie etwa PCI DSS für Kreditkarten und TISAX für Leistungen in der Automobilbranche.

Zertifizierungen nur ein Faktor der Vertrauensbildung

Wenn Zertifizierungen nicht durch externe Vorgaben fest vorgegeben sind, können sie zwar die Vertrauensbildung unterstützen. Dabei stellen sie aber nur einen Faktor dar. Andere Faktoren, wie Preis, Leistung, andere Referenzen, und Risikofaktoren, wie etwa der Standort der Verarbeitung, werden zumeist gleichberechtigt mitberücksichtigt.

Literaturangaben

Akerlof, G. A., 1979: The markets for lemons: Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 84. Jg., S. 488–500.

Behringer, S. & Passarge, M., 2020: Standards und Zertifikate für Compliance-Management-Systeme 2. Auflage. In: Compliance für KMU - Praxisleitfaden für den Mittelstand. Berlin: Erich Schmidt Verlag GmbH & Co. KG, S. 265 - 275.

Kersten, Heinrich, Klett, Gerhard, Reuters, Jürgen & Schröder, Klaus-Werner, 2020: IT-Sicherheitsmanagement nah der neuen ISO 27001. Wiesbaden: Springer Vieweg.

Lang, Michael, Wiesche, Manuel & Krcmar, Helmut, 2018: Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes. Information & Management, 9 März, S. 746-758.

Lang, Michael, Wiesche, Manuel & Krcmar, Helmut, 2018b: Möglichkeiten zum Nachweis vertrauenswürdiger Cloud Services. In: Management sicherer Cloud-Services - Entwicklung und Evaluation dynamischer Zertifikate. Wiesbaden: Springer Fachmedien Wiesbaden GmbH, S. 59-66.

Lins, Sebastian, 2019: Cloud-Service-Zertifizierung. München: Springer-Verlag GmbH.

Lins, Sebastian & Sunjaev, Ali, 2018: Klassifikation von Cloud-Services. In: Management sicherer Cloud-Services. Wiesbaden: Springer Fachmedien Wiesbaden GmbH, S. 8-13.

Klotz 2012: Klotz, Michael: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. 2., überarb. u. erw. Aufl. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2012 (SIMAT AP, 4 (2012), 20)

Marston, Sean, Li, Zhi, Bandyopadhyay, Subhajyoti, Zhang, Julie, 2011: Cloud computing – the business perspective. Decision Support Systems, April, S. 176-189.

Porath, Ron, 2020: Internet, Cyber- und IT-Sicherheit von A-Z, 2. Auflage. Wettswil, Schweiz: Springer Vieweg.

Schneider, Stephan., Lansing, Jens, Gao, Fangijan & Sunyaev, Ali, 2014: A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria. Waikoloa, HI, USA , Institute of Electrical and Electronics Engineers (IEEE), S. 4998-5007.

Schneider, Stephan & Sunyaev, Ali 2015: Cloud-Service-Zertifizierung - Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services. Berlin Heidelberg: Springer-Verlag.

Schneider, Stephan & Sunyaev, Ali, 2016: Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. Journal of Information Technology, 1 März, S. 1–32.

Sunyaev, Ali & Schneider, Stephan, 2013: Cloud services certification. Communications of the ACM 56, Februar, S. 33–36.

Traudes, Philipp, 2017: Zertifizierung und Compliance-Management Systeme. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.

Quellenangaben

Amazon, 2021: AWS-Compliance-Programme https://aws.amazon.com/de/compliance/programs/, zuletzt abgerufen am 11.04.2021.

Association of International Certified Professional Accountants (AICPA), 2016a: AT Section 801 - Reporting on Controls at a Service Organization, abgerufen von https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf , zuletzt am 11.04.2021.

Association of International Certified Professional Accountants (AICPA), 2016b: Attestation Standards: Clarification and Recodification, abgerufen von https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf, zuletzt am 11.04.2021.

Association of International Certified Professional Accountants (AICPA), 2018: CPAs: Helping service organizations build trust and transparency, abgerufen von https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-service-organizations-brochure.pdf, zuletzt am 11.04.2021.

Association of International Certified Professional Accountants (AICPA), 2020: TSP Section 100 - 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, abgerufen von https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf, zuletzt am 11.04.2021.

Booz & Company, 2012: Das Normungs- und Standardisierungsumfeld von Cloud Computing, Berlin: Booz & Company.

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019: Zertifizierungsschema für ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz, Bonn, Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020: Kriterienkatalog Cloud Computing, Bonn, Bundesamt für Sicherheit in der Informationstechnik.

Bundesministerium für Wirtschaft und Energie, 2021: Trusted Cloud, abgerufen von https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/trusted-cloud.html, zuletzt am 17.04.2021.

Cloud Security Alliance (CSA), 2019: CSA STAR Level and Scheme Requirements, abgerufen von https://cloudsecurityalliance.org/artifacts/star-level-and-scheme-requirements, zuletzt am 13.11.2020.

DAkkS, 2020: Online-Glossar der Webseite der Deutschen Akkreditierungsstelle. https://www.dakks.de/content/glossar , zuletzt abgerufen am 11.04.2021

ENX Association, 2021: TISAX-Teilnehmerhandbuch, Frankfurt am Main, abgerufen von https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf, zuletzt am 11.04.2021.

EuroCloud Deutschland_eco e.V (EuroCloud), 2019: STARAUDIT - Weltweite Nutzbarkeit auf der Basis europäischer Qualitätsstandards, abgerufen von https://www.eco.de/wp-

content/uploads/dlm_uploads/2019/04/staraudit_folder-de1.pdf, zuletzt am 11.04.2021.

Fedramp Programm Management Office, 2017: FedRAMP SECURITY ASSESSMENT FRAMEWORK, abgerufen von https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf , letzter Zugriff am 13.03.2021.

IBM, 2021: IBM Cloud compliance programs, https://www.ibm.com/cloud/compliance, zuletzt abgerufen am 11.04.2021.

Institut der Wirtschaftsprüfer in Deutschland e.V (IDW), 2013: Prüfungsstandard 951 „Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen, Düsseldorf

International Federation of Accountants (IFA), 2011: Auditing International Standard on Assurance Engagements (ISAE) 3402 – Assurance Reports on Controls at a Service Organization, abgerufen von https://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf, zuletzt am 17.04.2021.

International Organization for Standardization, 2020, The ISO Survey of Management System Standard Certifications – 2019 – Explanatory Note, abgerufen von https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1, zuletzt am 17.04.2021.

International Organization for Standardization / International Electrotechnical Commission, 2015: ISO 9001 Qualitätsmanagementsysteme - Anforderungen, Beuth Verlag.

International Organization for Standardization / International Electrotechnical Commission, 2015: 170021-1 Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren - Teil 1: Anforderungen, Beuth Verlag.

International Organization for Standardization / International Electrotechnical Commission, 2018: ISO 19011 Leitfaden zur Auditierung von Managementsystemen - Anforderungen, Beuth Verlag.

International Organization for Standardization / International Electrotechnical Commission, 2018: ISO/IEC 20000-1 Informationstechnik - Servicemanagement - Teil 1: Anforderungen an Servicemanagementsysteme, Beuth Verlag.

International Organization for Standardization / International Electrotechnical Commission, 2020: ISO 22301 Sicherheit und Resilienz - Business Continuity Management System – Anforderungen, Beuth Verlag

International Organization for Standardization / International Electrotechnical Commission, 2017, 27001 Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen, Beuth Verlag

Microsoft, 2021: Microsoft Compliance-Angebote, https://docs.microsoft.com/de-de/compliance/regulatory/offering-home, zuletzt abgerufen am 11.04.2021.

National Institute of Standards and Technology (NIST), 2011: Special Publication 800-145 - The NIST definition of cloud computing: recommendations of the national institute of standards and technology, abgerufen von https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, zuletzt am 11.04.2021.

National Institute of Standards and Technology (NIST), 2018: Framework for Improving Critical Infrastructure Cybersecurity, abgerufen von https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf , zuletzt am 11.04.2021.

National Institute of Standards and Technology (NIST), 2020: National Online Informative References(OLIR) Program, abgerufen von https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278.pdf, zuletzt am 17.04.2021.

HITRUST, 2020: HITRUST Certification of the NIST Cybersecurity Framework Certification https://hitrustalliance.net/certification/hitrust-certification-of-the-nist-cybersecurity-framework-certification/, zuletzt am 17.04.2021

PCI Security Standards Council, 2009: PCI Quick Reference Guide - Understanding the Payment Card Industry Data Security Standard v1.2, Wakefield, MA USA.

PCI Security Standards Council, 2018: PCI DSS Self-Assessment QuestionnaireInstructions and Guidelines, v3.2.1, Wakefield, MA USA.

Trusted Cloud Kompetenznetzwerk e.V., 2017: Vereinbarung über die Listung von Services auf dem Trusted Cloud Portal und die Nutzung des Labels Trusted Cloud, abgerufen von https://www.trusted-cloud.de/sites/default/files/trusted_cloud_vertrag_cloud_services_v2_0.pdf, zuletzt am 17.04.2021.

Trusted Cloud Kompetenznetzwerk e.V., 2018: Kriterienkatalog für Cloud Services, abgerufen unter https://www.trusted-cloud.de/sites/default/files/tc_kriterienkatalog_v2_final_2.pdf, zuletzt am 17.04.2021, Berlin, BMWi.

Trusted Cloud Kompetenznetzwerk e.V., 2020: Leitfaden zur Listung von Cloud Services und Anbietern Cloud-bezogener Dienstleistungen, abgerufen von https://www.trusted-cloud.de/index.php/de/artikel/listung-auf-trusted-cloud , zuletzt am 17.04.2021.

U.S. Department of Commerce 2021: Privacy Shield Overview, https://www.privacyshield.gov/Program-Overview, zuletzt abgerufen am 11.04.201.

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informations-arbeiter
01-09-003	09.2009	L. Ramin / M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop- Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Kaminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel / N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informationsmanage-ments
03-11-013	08.2011	H. Auerbach / N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesundheits-wirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutsch-sprachige Museums-Apps
03-11-016	11.2011	S. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Mecklenburg-Vorpommern – Strom als Wettbewerbsfaktor und Gegenstand der Standortvermarktung
04-12-017	04.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagementsoftware – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Inte-gration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.
04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA

AP	Datum	Autor	Titel
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	02.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen
06-14-025	01.2014	M. Klotz	IT-Compliance nach COBIT® – Gegenüberstellung von COBIT® 4.0 und COBIT® 5
06-14-026	04.2014	L. von Blumröder	Projektpriorisierung im Rahmen eines ganzheitlichen Projektportfoliomanagements
06-14-027	06.2014	S. Press	Automatisierte Kontrollen in der Beschaffung – Exemplarische Konzeption und Umsetzung
06-14-028	07.2014	M. Klotz	IT-Compliance – Begrifflichkeit und Grundlagen
07-15-029	09.2015	M. Klotz	Projektmanagement-Normen und -Standards
08-16-030	08.2016	M. Klotz	ISO/IEC 3850x – Die Normenreihe zur IT-Governance
09-17-031	09.2017	S. Marx	Project Management Practice in Interreg Projects – Reflective Analysis and Recommendations
09-17-032	11.2017	S. Marx	Knowledge Management in Interreg Cross-Border Cooperation – a Project Perspective
10-18-033	11.2018	M. Klotz / S. Marx	Projektmanagement-Normen und -Standards, 2. Aufl.
11-19-034	08.2019	M. Klotz	IT-Compliance nach COBIT® 2019
11-19-035	09.2019	I. Sulk / P. Hagen / M. Klotz	Kontrollanforderungen an ein ERP/Cloud-System und Umsetzung in automatisierte Kontrollen
12-20-036	03.2020	S. Marx / M. Klotz	Earned-Value-Analyse – Einführung und Beispiele
12-20-037	04.2020	M. Kenter / C. Bülow / M. Weber / L. Kennes	Lebensqualität in Vorpommern-Rügen – Ein Vergleich mit ausgewählten Metropolen und Vergleichsstädten Deutschlands
12-20-038	05.2020	S. Marx / M. Klotz	Hackathons in Museums – Recommendations from an International Event Series
13-21-039	03.2021	M. Naybzadeh	Standards und Zertifizierungen für Cloud-Services