

Cloud Computing

Eine Orientierungshilfe für Cloud-Service-Kunden



Inhaltsverzeichnis

EINLEITUNG	4
1. CLOUD-GRUNDLAGEN	6
1.1. Rollen und Aufgaben	6
1.2. Hauptmerkmale.....	7
1.3. Betriebsmodelle.....	8
1.4. Servicemodelle	10
1.5. Querschnittsaspekte	11
1.6. Fazit	13
2. STRATEGISCHE PLANUNG	14
2.1. Vorgehensweise	14
2.1.1. Planungsschritte	14
2.1.2. Planungsaspekte	15
2.2. Schutzbedarfsfeststellung	16
2.2.1. Schutzbedarfskategorien	16
2.2.2. Schadensszenarien.....	17
2.2.3. Datenkategorien	17
2.2.4. Einstufungsmodell.....	18
2.3. Bedarfsanalyse.....	20
2.3.1. Rechtliche Rahmenbedingungen	20
2.3.2. Betriebliche Rahmenbedingungen	24
2.3.3. Zertifizierungsstandards	27
2.3.4. Prüfungsstandards	28
2.3.5. Gütesiegel	29
2.4. Risikoanalyse	29
2.4.1. Prozesselemente	30
2.4.2. Risikoidentifikation	31
2.4.3. Risikoabschätzung und -auswertung.....	32
2.4.4. Risikobewältigung	33
2.5. Datenschutz-Folgenabschätzung	34
2.5.1. Prozesselemente	34
2.5.2. Relevanzschwelle	36
2.5.3. Anforderungen.....	37
2.5.4. Besonderheiten.....	37
2.5.5. Kriterien	39
2.6. Fazit	40
3. ANFORDERUNGSSPEZIFIKATION	41
3.1. Anforderungskriterien	41
3.2. Vertragliche Rahmenbedingungen	43
3.2.1. Vertragspartner	43
3.2.2. Vertragslaufzeit und -änderungen	45
3.2.3. Vertragsbeendigung und -streitigkeiten	47
3.3. Vertragsgegenstand	49
3.3.1. Allgemeine Vereinbarungen	49
3.3.2. Vereinbarungen zur Servicequalität	54
3.3.3. Vereinbarungen zur Informationssicherheit.....	60
3.3.4. Vereinbarungen zum Datenschutz	75
3.4. Fazit	80

4.	WEITERFÜHRENDE INFORMATIONEN	81
4.1.	Organisationen	81
4.2.	Cloud-Grundlagen	82
4.3.	Cloud-Strategie	83
4.4.	Rechtsvorschriften	83
4.5.	Datenschutzrechtliche Orientierungshilfen	85
4.6.	E-Government-Konventionen	85
4.7.	Zertifizierungsstandards	86
4.8.	Prüfungsstandards	87
4.9.	Gütesiegel	88
4.10.	Servicestandards	88
4.10.1.	Anforderungen an Cloud-Services	88
4.10.2.	IT-Service-Management	88
4.10.3.	Service Level Agreements	89
4.10.4.	Interoperabilität und Portabilität	89
4.11.	Sicherheitsstandards	90
4.11.1.	Anforderungen an Cloud-Services	90
4.11.2.	Informationssicherheitsmanagement	90
4.11.3.	Risikomanagement	91
4.11.4.	Auditierung und Test	92
4.11.5.	Sicherheitsschwachstellenmanagement	92
4.11.6.	Sicherheitsvorfallmanagement	93
4.11.7.	Business Continuity Management	93
4.11.8.	Applikationssicherheit	93
4.11.9.	Identity- und Access-Management	94
4.11.10.	Kryptografie	95
4.11.11.	Systemhärtung	98
4.11.12.	Datenlöschung	99
4.11.13.	Systemevaluierung	99
4.11.14.	Rechenzentren	100
4.11.15.	Weitere technische Spezifikationen	101
4.12.	Datenschutzstandards	101
4.12.1.	Anforderungen an Cloud-Services	101
4.12.2.	Datenschutzmanagement	102
4.12.3.	Datenschutzfolgenabschätzung	102
4.12.4.	Privacy Level Agreements	102
4.12.5.	Rahmenwerke, Handbücher und Kataloge	102
4.13.	Fazit	103
	ABKÜRZUNGSVERZEICHNIS	104

Einleitung

Cloud Computing ist bereits in vielen Bereichen des gesellschaftlichen und wirtschaftlichen Lebens angekommen. Das immer breiter werdende Spektrum an Cloud-Services hat sich zu einer echten Alternative entwickelt. Dennoch ist deren Einsatz nicht in allen Fällen die bessere Lösung. Ob bei einer Verwendung von Cloud-Services die Vorteile überwiegen, hängt vom jeweiligen Einsatzszenario und dessen technischen, organisatorischen und rechtlichen Anforderungen ab. Das Herbeiführen einer Entscheidung für oder gegen eine Verwendung von Cloud-Services ist aufgrund der vielen zu beachtenden Aspekte ein komplexes Unterfangen.

Der Cloud Computing Kompass versteht sich als neutrale und objektive Orientierungshilfe, die Cloud-Service-Kunden im privaten sowie im öffentlichen Bereich bei der Bewältigung der Herausforderungen, die sich aus einer Verwendung von Cloud-Services ergeben, unterstützen soll. Die Inhalte gliedern sich in die vier dargestellten Bereiche, welche unterschiedliche Aspekte der Vorgehensweise abdecken.



Abbildung 1: Struktur und Vorgehensweise

Um die Verwendung von Cloud Computing prinzipiell in Erwägung ziehen zu können, sind grundlegende Kenntnisse über dieses Modell notwendig. Abschnitt 1 gibt daher einen allgemeinen Überblick über das Modell und führt zentrale Begriffe und Konzepte ein. Damit richtet sich dieser Abschnitt vor allem an jene Personen, die Grundkenntnisse über Cloud Computing erwerben möchten, um die Potenziale dieses Modells für ihre eigenen Anwendungsfälle besser abschätzen zu können.

Die Entscheidung für einen Einsatz von Cloud-Services in der Organisation sollte immer auf Grundlage einer strategischen Planung erfolgen, im Rahmen derer eine Schutzbedarfsfeststellung, eine Bedarfs- und Risikoanalyse und erforderlichenfalls eine Datenschutzfolgenabschätzung durchgeführt und alle entscheidenden Fragen geklärt wurden. Abschnitt 0 unterstützt bei der systematischen Vorgehensweise und Berücksichtigung wesentlicher Planungsaspekte die fundierte Entscheidungsfindung.

Ist die Entscheidung für eine Verwendung von Cloud-Services erst einmal getroffen, folgt im nächsten Schritt die Auswahl eines passenden Cloud-Service-Providers und die Vertragsgestaltung mit diesem. Dafür sollten mit dem Cloud-Service-Provider konkrete Anforderungen festgelegt und vertraglich vereinbart werden. Zur Sicherstellung einer ausreichenden Qualität und Angemessenheit der Anforderungen unterstützt Abschnitt 3 bei der Auswahl und Spezifikation wesentlicher Anforderungskriterien.

Cloud Computing erfordert die Berücksichtigung einer Vielzahl unterschiedlicher technischer, organisatorischer und rechtlicher Aspekte. Der Cloud Computing Kompass versucht zwar, diese Aspekte möglichst umfassend zu beleuchten, erhebt aber keinen Anspruch auf Vollständigkeit. Da aufgrund der Komplexität des Themas nicht alle Bereiche im Detail behandelt werden können, stellt Abschnitt 3.4 eine umfassende Auswahl weiterführender Informationen zur Verfügung, die eine Vertiefung in die Materie und ein gezieltes Erarbeiten von Detailwissen zu speziellen Teilbereichen ermöglichen soll.

Der Cloud Computing Kompass wurde von A-SIT Plus und dem Bundesministerium für Finanzen auf Grundlage der nachfolgend abgebildeten internationalen Standards erstellt. Die Ausarbeitung erfolgte im Rahmen eines KIRAS Sicherheitsforschungsprojekts in Zusammenarbeit mit EuroCloud Austria, IDC und Repuco.

Begriffe und Architektur

- ISO/IEC 17788 – Cloud Computing – Übersicht und Vokabular
- ISO/IEC 17789 – Cloud Computing – Referenzarchitektur

Informationssicherheit

- ISO/IEC 27001 – Informationssicherheits- Managementsysteme – Anforderungen
- ISO/IEC 27017 – Leitfaden – Informationssicherheitsmaßnahmen für Cloud-Services

Service-Management

- ISO/IEC 20000-1 – Service-Management – Systemanforderungen
- ISO/IEC 20000-9 – Service-Management – Leitfaden für Cloud-Services

Datenschutz

- ISO/IEC 29151 – Leitfaden – Datenschutz
- ISO/IEC 27018 – Leitfaden – Datenschutz in Public Cloud-Services

1. Cloud-Grundlagen

Cloud Computing ist ein Modell, das einen bedarfsorientierten und netzwerkbasierten Zugriff auf einen skalierbaren und elastischen sowie selbst provisionierbaren und administrierbaren Pool von geteilten physischen oder virtuellen Ressourcen ermöglicht. Dazu zählen beispielsweise Server, Betriebssysteme, Netzwerke, Software, Applikationen und Speichersysteme. Der Begriff Cloud Computing umfasst ein breites Spektrum entsprechender Lösungen, die sich wiederum in diverse Unterkategorien klassifizieren lassen.

Dieser Abschnitt stellt die wichtigsten dieser Kategorien vor und führt dabei einige für Cloud Computing zentrale Begriffe und Konzepte ein. Damit bietet dieser Abschnitt jenen Personen einen einfachen Einstieg in die Materie, die mit Cloud Computing bisher nur wenig Erfahrung sammeln konnten.

1.1. Rollen und Aufgaben

Im Sinne einer einheitlichen Notation ist es zunächst sinnvoll, die für Cloud Computing zentralen Rollen zu definieren. Die ISO/IEC Norm 17788 unterscheidet diesbezüglich ganz allgemein die drei folgenden Rollen mit jeweils unterschiedlichen zugeordneten Aufgabenbereichen.

Cloud-Service-Kunden

Cloud-Service-Kunden haben ein Vertragsverhältnis mit Cloud-Service-Providern oder Cloud-Service-Partnern, das sich auf die Nutzung von Cloud-Services bezieht. Ihre Hauptaufgaben liegen insb. in der Nutzung und Verwaltung von Cloud-Services zur Abwicklung ihrer Geschäftsprozesse.

Cloud-Service-Provider

Cloud-Service-Provider haben ein Vertragsverhältnis mit Cloud-Service-Kunden oder Cloud-Service-Partnern, das sich auf die Bereitstellung von Cloud-Services bezieht. Ihre Hauptaufgaben liegen insb. im Betrieb und in der Wartung von Cloud-Infrastrukturen zur Bereitstellung von Cloud-Services.

Cloud-Service-Partner

Cloud-Service-Partner haben ein Vertragsverhältnis mit Cloud-Service-Providern oder Cloud-Service-Kunden, das sich auf deren Betreuung oder Unterstützung bezieht. Beispiele für Cloud-Service-Partner sind Cloud-Auditoren und Cloud-Makler.

1.2. Hauptmerkmale

Cloud Computing gleicht zwar in einigen Punkten dem Modell des klassischen IT-Outsourcings, bei dem Geschäftsprozesse ganz oder teilweise an externe IT-Dienstleister ausgelagert werden. In Summe bestehen zwischen den beiden Modellen jedoch wesentliche Unterschiede. Generell charakterisiert sich Cloud Computing durch folgende Hauptmerkmale.

Umfassender Netzwerkzugriff

Der Zugriff auf die physischen und virtuellen Ressourcen erfolgt mittels Standard-Mechanismen und unterstützt dadurch heterogene Client-Plattformen.

Mandantenfähigkeit

Die Zuweisung der physischen und virtuellen Ressourcen erfolgt auf eine Art, dass mehrere Cloud-Service-Kunden und ihre Datenverarbeitung voneinander getrennt und untereinander nicht zugänglich sind.

Rasche Elastizität und Skalierbarkeit

Um die physischen und virtuellen Ressourcen schnell zu erhöhen oder zu reduzieren, können diese rasch und elastisch angepasst werden, in einigen Fällen auch automatisch.

Service-orientierte Architektur (SOA)

SOA ist eine der Grundvoraussetzungen für Cloud Computing. Die Cloud-Services werden in der Regel über ein sogenanntes REST-API angeboten.

Servicevermessung

Die Servicevermessung ermöglicht eine Ressourcennutzung, die entsprechend überwacht, kontrolliert, berichtet und verrechnet werden kann.

Bedarfsgerechte Selbst-Provisionierung

Die bedarfsgerechte Bereitstellung der physischen und virtuellen Ressourcen durch den Cloud-Service-Kunden erfolgt automatisch oder mit minimaler Interaktion mit dem Cloud-Service-Provider.

Aggregation der Ressourcen

Die physischen und virtuellen Ressourcen des Cloud-Service-Providers können aggregiert werden, um einen oder mehrere Cloud-Service-Kunden zu bedienen.

Nutzungsgerechte Verrechnung

Es werden nur Ressourcen bezahlt, die tatsächlich in Anspruch genommen wurden (Pay per Use Model), wobei es auch Flatrate-Modelle geben kann.

In Fachkreisen werden darüber hinaus folgende weitere Eigenschaften genannt.

1.3. Betriebsmodelle

Der Einfluss, den Cloud-Service-Kunden auf die Steuerung und Kontrolle von verwendeten Cloud-Services haben, hängt stark vom zugrundeliegenden Betriebsmodell des jeweiligen Cloud-Services ab. Neben den Urformen Public Cloud und Private Cloud existieren mittlerweile weitere Betriebsmodelle wie Community Cloud, Virtual Private Cloud und Hybrid Cloud.

Private Cloud

Eine Private Cloud wird exklusiv durch einen einzelnen Cloud-Service-Kunden genutzt. Der Cloud-Service-Kunde kann bei Bedarf weiteren Organisationen (wie z. B. Partnern, Lieferanten und Kunden) einen Zugang ermöglichen.

Virtual Private Cloud

Eine Virtual Private Cloud ist ein Spezialfall einer Public Cloud, bei der mittels geeigneter Sicherheitsmechanismen eine abgeschottete und individualisierte Serviceumgebung bereitgestellt wird. Diese wird – wie eine Private Cloud – exklusiv durch einen einzelnen Cloud-Service-Kunden genutzt.

Hybrid Cloud

Eine Hybrid Cloud nutzt mindestens zwei verschiedene und eigenständige Betriebsmodelle, die über standardisierte Schnittstellen miteinander verbunden sind und eine entsprechende Interoperabilität und Portabilität ermöglichen.

Community Cloud

Eine Community Cloud wird exklusiv durch eine Gemeinschaft bestimmter Cloud-Service-Kunden mit gemeinsamen Anforderungen und Interessen genutzt.

Public Cloud

Eine Public Cloud kann potenziell durch beliebige Cloud-Service-Kunden genutzt werden. Sie wird üblicherweise von Unternehmen oder von privaten oder öffentlichen Organisationen bereitgestellt.

Die nachfolgende Tabelle beschreibt die wesentlichen Unterschiede der einzelnen Betriebsmodelle hinsichtlich Erreichbarkeit, Ressourcen-Management, Betrieb, Lokation, Sourcing-Optionen und Vertragsgestaltung.

Die Angaben in der Tabelle basieren im Wesentlichen auf den Inhalten der ISO/IEC Normen 17788 und 17789.

PRIVATE CLOUD	COMMUNITY CLOUD	VIRTUAL PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD
Cloud-Service-Erreichbarkeit				
i. d. R. über ein Intranet oder ein Virtual Private Network eingeschränkt			i. d. R. öffentlich über das Internet verfügbar	abhängig vom Betriebsmodell
Cloud-Service-Zugriff				
erfolgt mittels Client (z. B. Web-Browser) auf IaaS-, PaaS- und SaaS-Services				
Cloud-Service-Ressourcen-Management				
erfolgt durch den Cloud-Service-Kunden	erfolgt durch einen oder mehrere Cloud-Service-Kunden der Gemeinschaft	erfolgt durch den Cloud-Service-Kunden	erfolgt durch den Cloud-Service-Provider	abhängig vom Betriebsmodell
Eigentümer und Betreiber der Cloud-Service-Infrastruktur				
ist der Cloud-Service-Kunde selbst oder ein Dritter	ist bzw. sind ein oder mehrere Cloud-Service-Kunde/n der Gemeinschaft , ein Dritter oder eine Kombination daraus	ist der Cloud-Service-Provider		abhängig vom Betriebsmodell
Lokation der Cloud-Service-Infrastruktur				
aus Sicht des Cloud-Service-Kunden On-Premise oder Off-Premise		aus Sicht der Cloud-Service-Kunden Off-Premise		abhängig vom Betriebsmodell
Sourcing-Optionen aus Sicht des Cloud-Service-Kunden				
outsourced, managed, insourced		outsourced		abhängig vom Betriebsmodell
Cloud-Service-Vertrag				
ist i. d. R. individuell definierbar	ist i. d. R. eingeschränkt anpassbar		ist i. d. R. nicht individuell anpassbar	abhängig vom Betriebsmodell

Tabelle 1: Unterschiede zwischen den Cloud Computing-Betriebsmodellen

1.4. Servicemodelle

Für den Einfluss des Cloud-Service-Kunden auf bereitgestellte Cloud-Services ist das jeweilige Servicemodell ausschlaggebend. Konkret beschreibt das Servicemodell, auf welcher Ebene (Software, Plattform, Infrastruktur etc.) Cloud-Service-Kunden Zugriff auf bereitgestellte Cloud-Services haben. Die Einteilung erfolgt grundsätzlich in die Servicemodelle Software as a Service, Platform as a Service und Infrastructure as a Service.

Software as a Service (SaaS)

Software as a Service ist die Bereitstellung von IT-Anwendungen, wie z. B. Office- und Kollaborationsanwendungen, in Form von Cloud-Services, die von Cloud-Service-Kunden genutzt werden können. Die Kontrolle über alle Ebenen liegt beim Cloud-Service-Provider.

Infrastructure as a Service (IaaS)

Infrastructure as a Service ist die Bereitstellung von IT-Infrastrukturressourcen, wie z. B. Rechenleistung, Speicher- und Netzwerksysteme, in Form von Cloud-Services, die Cloud-Service-Kunden zur Bereitstellung eigener Services nutzen können. Die Kontrolle der Cloud-Service-Kunden reicht vom Betriebssystem aufwärts.

Darüber hinaus konnten sich in den letzten Jahren weitere artverwandte Modelle wie Containerisierung etablieren.

Der Begriff „as a Service“ wird mittlerweile für eine Vielzahl weiterer Cloud-Service-Angebote genutzt, wie z. B.:

- Communications as a Service
- Compute as a Service
- Database as a Service
- Data Storage as a Service
- Desktop as a Service
- Federation as a Service
- E-Mail as a Service
- Identity as a Service
- Management as a Service
- Network as a Service
- Security as a Service

Platform as a Service (PaaS)

Platform as a Service ist die Bereitstellung von kompletten IT-Plattformen in Form von Cloud-Services, die Cloud-Service-Kunden zur Bereitstellung eigener IT-Anwendungen nutzen können. Die Kontrolle der Cloud-Service-Kunden beschränkt sich auf die Anwendungsebene.

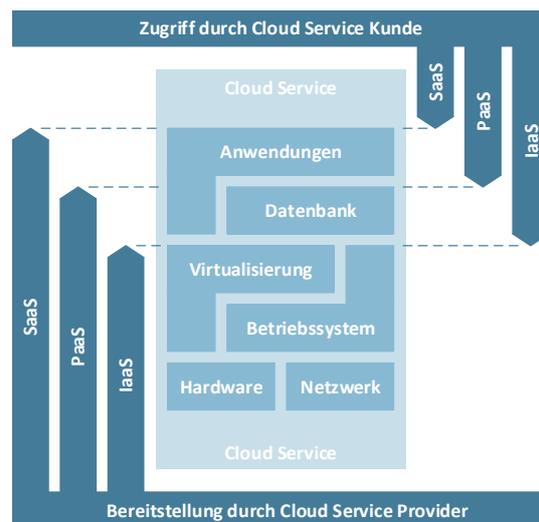


Abbildung 2: Cloud Computing-Servicemodelle

1.5. Querschnittsaspekte

Die ISO/IEC Norm 17788 beschreibt zudem relevante Querschnittsaspekte in Form von Eigenschaften und Fähigkeiten, die im Zusammenhang mit Cloud Computing von Bedeutung sind.

Auditierbarkeit

Auditierbarkeit bezeichnet die Fähigkeit, erforderliche Nachweise im Zusammenhang mit dem Betrieb und der Nutzung von Cloud-Services zu sammeln, evident zu halten und bei Prüfungen vorzulegen.

Datenschutz

Datenschutz umfasst den Schutz von personenbezogenen Daten bei der Ermittlung, Verarbeitung, Kommunikation, Nutzung und Vernichtung in einer garantierten, korrekten und konsistenten Form.

Governance

Governance bezeichnet die Regelungen und Prozesse zur Steuerung und Kontrolle der Bereitstellung und Nutzung von Cloud-Services mittels Service Level Agreements und anderer vertraglicher Vereinbarungen.

Leistungsfähigkeit

Leistungsfähigkeit umfasst alle Betriebsparameter von Cloud-Services, die im Service Level Agreement vereinbart wurden.

Rückführbarkeit

Rückführbarkeit bezeichnet die Fähigkeit der Rückgabe aller Daten und Applikationen an den Cloud-Service-Kunden und die Löschung aller Daten und Ergebnisse durch den Cloud-Service-Provider innerhalb der vereinbarten Frist.

Compliance

Compliance bezeichnet die Einhaltung von gesetzlichen, vertraglichen und sonstigen regulatorischen Vorgaben im Rahmen des Betriebs und der Nutzung von Cloud-Services.

Resilienz

Resilienz bezeichnet die Fähigkeit von Cloud-Services, im Fehlerfall eine ausreichende Dienstgüte aufrechtzuerhalten.

Interoperabilität

Interoperabilität bezeichnet die Fähigkeit von Cloud-Services mit anderen Systemen zu interagieren und Informationen in einer festgelegten Form auszutauschen, um vorhersagbare Ergebnisse zu erhalten.

Portierbarkeit

Portierbarkeit bezeichnet die Fähigkeit von Cloud-Services, Daten und Applikationen kostengünstig und kurzfristig zwischen verschiedenen Cloud-Service-Providern zu portieren.

Service Level Agreements (SLA)

Service Level Agreements sind Vereinbarungen zwischen Cloud-Service-Provider und Cloud-Service-Kunden über die zu erbringende Dienstgüte von Cloud-Services in Form von messbaren Eigenschaften.

Sicherheit

Sicherheit – oder Informationssicherheit – bezeichnet das Spektrum von physischer Sicherheit bis hin zur Applikationssicherheit von Cloud-Services, einschl. Authentifizierung, Autorisierung, Verfügbarkeit, Vertraulichkeit, Identitätsmanagement, Integrität, Nichtabstreitbarkeit, Audit, Sicherheitsmonitoring, Reaktion auf Sicherheitsvorfälle und Security Policy Management.

Verfügbarkeit

Verfügbarkeit bezeichnet die Eigenschaft von Cloud-Services bei Bedarf für eine autorisierte Entität erreichbar und nutzbar zu sein.

Wartung und Versionierung

Wartung betrifft Änderungen aufgrund von Fehlerbehebungen, Serviceupdates und Funktionserweiterungen; Versionierung die angemessene Kennzeichnung einer bestimmten Version.

Bei einer generellen Bewertung der Betriebsmodelle hinsichtlich ihrer Eignung im Zusammenhang mit den genannten Querschnittsaspekten ergibt sich – insb. bei hohen Anforderungen – eine Präferenz zur Implementierung von Private Clouds und Community Clouds. Selbstverständlich kann dies im Einzelfall variieren. Die nachfolgende Tabelle verdeutlicht dies.

PRIVATE CLOUD	COMMUNITY CLOUD	VIRTUAL PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD
Auditierbarkeit				
●	◐	◐	○	◐
Compliance¹				
●	●	◐	○	◐
Datenschutz¹				
●	●	◐	○	◐
Resilienz				
●	●	●	●	●
Governance				
●	◐	○	○	◐
Interoperabilität				
●	◐	◐	○	◐
Leistungsfähigkeit				
●	●	●	●	●
Portierbarkeit				
●	●	◐	◐	◐

Tabelle 2: Generelle Bewertung der Betriebsmodelle (Teil 1)

PRIVATE CLOUD	COMMUNITY CLOUD	VIRTUAL PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD
Rückführbarkeit				
●	●	◐	◐	◐
Service Level Agreements				
●	●	●	◐	◐
Sicherheit¹⁾				
●	●	◐	○	◐
Verfügbarkeit				
●	●	●	●	●
Wartung und Versionierung				
●	●	●	●	●

Tabelle 3: Generelle Bewertung der Betriebsmodelle (Teil 2)

¹⁾ betrifft die Kontrolle durch den Cloud-Service-Kunden

● hohe Eignung

◐ eingeschränkte Eignung

○ geringe Eignung

Die in der Tabelle angeführten Werte beruhen auf allgemein anerkannten Eigenschaften der einzelnen Betriebsmodelle bzw. leiten sich aus Angaben aus den ISO/IEC Normen 17788 und 17789 ab. Durch das gewählte dreistufige Bewertungsschema kann sich hier für einzelne Aspekte naturgemäß eine Unschärfe ergeben, die Kernaussage in Bezug auf die Präferenz von Private Clouds und Community Clouds bleibt davon jedoch unberührt.

1.6. Fazit

Cloud Computing beschreibt weniger eine spezielle Technologie als vielmehr ein generisches Modell für den bedarfsorientierten und netzwerkbasierten Zugriff auf einen skalierbaren und elastischen sowie selbst provisionierbaren und administrierbaren Pool von geteilten physischen oder virtuellen Ressourcen. Relevante Unterkategorien lassen sich dabei etwa anhand des zugrundeliegenden Betriebsmodells oder Servicemodells bilden.

Unabhängig vom jeweiligen Modell bleiben jedoch die Hauptmerkmale von Cloud Computing wie Mandantenfähigkeit, Elastizität oder auch nutzungsgerechte Verrechnung häufig bestehen. Damit stellt Cloud Computing eine attraktive Lösung für eine Vielzahl unterschiedlichster Anwendungsfälle dar. Relevante Aspekte für die strategische Planung des Einsatzes von Cloud Computing für einen gegebenen Anwendungsfall werden im folgenden Abschnitt im Detail beleuchtet.

2. Strategische Planung

Bevor Daten und Datenanwendungen in die Cloud ausgelagert werden, ist die Durchführung einer strategischen Planung unbedingt anzuraten. Diese Planung sollte eine Schutzbedarfsfeststellung, eine Bedarfs- und Risikoanalyse und erforderlichenfalls eine Datenschutzfolgenabschätzung umfassen. Die Planungsergebnisse bilden letztendlich die Grundlage für eine fundierte Entscheidung, ob und in welcher Form Cloud-Services für den gegebenen Anwendungsfall eingesetzt werden können.

Dieser Abschnitt behandelt die wichtigsten Aspekte einer solchen strategischen Planung und unterstützt damit bei der Herbeiführung einer Entscheidung über den Einsatz von Cloud Computing für einen gegebenen Anwendungsfall.

2.1. Vorgehensweise

2.1.1. Planungsschritte

Die strategische Planung liefert wichtige Entscheidungsgrundlagen für oder gegen eine Verwendung von Cloud Computing. Sie sollte daher für jeden Anwendungsfall systematisch durchlaufen werden und zumindest die folgenden Planungsschritte enthalten.

1. Schutzbedarfsfeststellung

Zuallererst ist der Schutzbedarf der auszulagernden Daten und Datenanwendungen anhand von Schutzbedarfskategorien, Schadensszenarien und Datenkategorien einzustufen.

3. Risikoanalyse

Im nächsten Schritt sind die bestehenden Informationssicherheitsrisiken aus Sicht des Cloud-Service-Kunden zu identifizieren und zu analysieren sowie geeignete Sicherheitsmaßnahmen zur Risikoreduzierung festzulegen.

2. Bedarfsanalyse

Im zweiten Schritt sind die vorliegenden rechtlichen und betrieblichen Rahmenbedingungen in Bezug auf die auszulagernden Daten und Datenanwendungen zu erheben bzw. festzulegen.

4. Datenschutzfolgenabschätzung

Liegen die Voraussetzungen für eine Datenschutzfolgenabschätzung vor, sind abschließend die bestehenden Datenschutzrisiken aus Sicht der Betroffenen zu analysieren und gegebenenfalls weitere Sicherheitsmaßnahmen festzulegen.

2.1.2. Planungsaspekte

Bei der strategischen Planung sind zahlreiche Aspekte zu klären, die in weiterer Folge in die Anforderungsspezifikation einfließen, wie z. B. Compliance-, Qualitäts-, Sicherheits- und Datenschutzaspekte. Die nachfolgende Abbildung gibt einen Überblick über die wesentlichen Aspekte und Bereiche, die im Zuge der strategischen Planung berücksichtigt werden müssen.

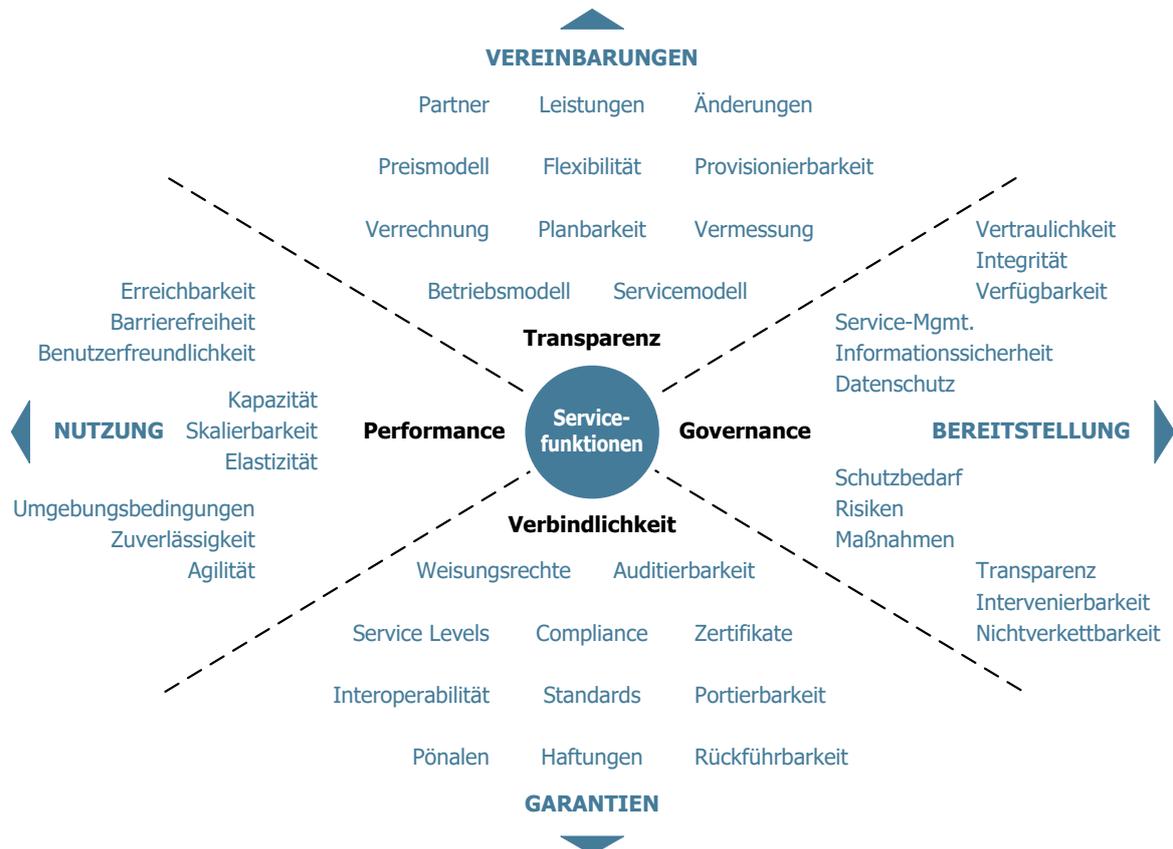


Abbildung 3: Planungsaspekte

Die Komplexität der Abbildung verdeutlicht das sehr breite Spektrum an Aspekten, die im Rahmen der strategischen Planung von Bedeutung sind. Es ist unumgänglich, dass diese Aspekte in allen Einzelschritten der strategischen Planung, die in den folgenden Unterabschnitten beschrieben werden, geeignet berücksichtigt werden.

2.2. Schutzbedarfsfeststellung

Der erste Schritt der strategischen Planung ist die Schutzbedarfsfeststellung. Diese dient der Ermittlung des angemessenen Schutzbedarfs der auszulagernden Daten und Datenanwendungen. Der Schutzbedarf orientiert sich an den möglichen Schäden, die bei einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Datenanwendungen sowie der betroffenen Geschäftsprozesse der Organisation zu erwarten sind.

Für die Schutzbedarfsfeststellung ist ein Einstufungsmodell mit Schutzbedarfskategorien, Schadensszenarien und Datenkategorien festzulegen. Das hier abgebildete Modell basiert auf den Empfehlungen des Österreichischen Informationssicherheitshandbuchs. Eine detaillierte Vorgehensweise wird auch im BSI-Standard 100-2 beschrieben. ➔ [Informationssicherheitsmanagement](#)

2.2.1. Schutzbedarfskategorien

Die Anzahl der erforderlichen Schutzbedarfskategorien ist von den Rahmenbedingungen der Organisation abhängig. Der Cloud Computing Kompass verwendet ein repräsentatives vierstufiges Modell. Je nach Anwendungsfall kann eine Adaptierung des Modells sinnvoll sein, etwa um bei Bedarf eine höhere Granularität zu erreichen. In der Regel sollten die unten angeführten vier Schutzbedarfskategorien jedoch ausreichend sein.

Stufe 1 – UNKRITISCH

Die Schadensauswirkungen aufgrund von Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit sind minimal und tolerierbar.

Stufe 3 – HOCH

Die Schadensauswirkungen aufgrund von Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit sind beträchtlich und keinesfalls tolerierbar.

Stufe 2 – NORMAL

Die Schadensauswirkungen aufgrund von Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit sind begrenzt und überschaubar und teilweise noch tolerierbar.

Stufe 4 – SEHR HOCH

Die Schadensauswirkungen aufgrund von Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit können ein existenziell bedrohliches bzw. katastrophales Ausmaß erreichen.

2.2.2. Schadensszenarien

So wie die oben beschriebenen Schutzbedarfskategorien sind auch Art und Anzahl der betrachteten Schadensszenarien von den Rahmenbedingungen der Organisation abhängig und daher bei Bedarf anzupassen. Als Basis können die im Folgenden angeführten Schadensszenarien herangezogen werden.

Compliance

Verstoß gegen Gesetze, Vorschriften und Verträge

Datenschutz

Beeinträchtigung des informationellen Selbstbestimmungsrechts

Gesundheit

Beeinträchtigung der persönlichen körperlichen Unversehrtheit

Geschäftsprozesse

Beeinträchtigung der Aufgabenerfüllung der Organisation

Image und Vertrauen

Negative Innen- oder Außenwirkung

Finanziell

Direkte oder indirekte finanzielle Auswirkungen

2.2.3. Datenkategorien

Bei der Ermittlung des Schutzbedarfs hat sich auch die Festlegung von Datenkategorien bewährt. Auch diese sind von der Organisation abhängig und dementsprechend individuell auszuwählen. Der Cloud Computing Kompass verwendet folgende Datenkategorien, die in der Praxis auch für viele Organisationen ausreichend sein sollten.

Öffentliche Daten

Dazu zählen Daten, die zur Veröffentlichung bestimmt sind, wie z. B. öffentliche Webseiten.

Personenbezogene Daten

Dazu zählen personenbezogene Daten gem. Art. 4 Z 1 DSGVO, besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO und personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO.

Interne Daten

Dazu zählen organisationsinterne Daten, die nicht zur Veröffentlichung bestimmt sind sowie Daten, die gesetzlichen Geheimhaltungspflichten unterliegen, insb. Amts-, Berufs-, Geschäfts- und Betriebsgeheimnisse.

Verschlusssachen

Dazu zählen Informationen gem. InfoSiG bzw. GehSO und Staatsgeheimnisse.

2.2.4. Einstufungsmodell

Das nachfolgende Modell basiert auf den definierten Schutzbedarfskategorien und dient zur Orientierung. Auch hier ist bei Bedarf eine Anpassung vorzunehmen.

Stufe 1 – UNKRITISCH

Betroffene Datenkategorien	▪ Öffentliche Daten
Verstoß gegen Gesetze, Vorschriften und Verträge	▪ Nicht möglich
Beeinträchtigung des informationellen Selbstbestimmungsrechts	▪ Nicht möglich
Beeinträchtigung der persönlichen Unversehrtheit	▪ Nicht möglich
Beeinträchtigung der Aufgabenerfüllung	▪ Geringfügig und tolerierbar ▪ Zielerreichung weiterhin möglich
Negative Innen- oder Außenwirkung	▪ Unbedeutende Ansehens- oder Vertrauensbeeinträchtigung
Finanzielle Auswirkungen	▪ Unbedeutend und tolerierbar

Stufe 2 – NORMAL

Betroffene Datenkategorien	▪ Interne Daten ▪ Personenbezogene Daten gem. Art. 4 Z 1 DSGVO
Verstoß gegen Gesetze, Vorschriften und Verträge	▪ Geringfügige Konsequenzen ▪ Geringe Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	▪ Personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann
Beeinträchtigung der persönlichen Unversehrtheit	▪ Nicht zulässig
Beeinträchtigung der Aufgabenerfüllung	▪ Geringfügig und tolerierbar ▪ Zielerreichung ist mit vertretbarem Mehraufwand möglich
Negative Innen- oder Außenwirkung	▪ Geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung
Finanzielle Auswirkungen	▪ Gering und tolerierbar

Stufe 3 – HOCH

Betroffene Datenkategorien	<ul style="list-style-type: none">▪ Personenbezogene Daten gem. Art. 4 Z 1 DSGVO, wobei die Betroffenen von den Entscheidungen bzw. Leistungen der Organisation abhängig sind▪ Besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO▪ Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO
Verstoß gegen Gesetze, Vorschriften und Verträge	<ul style="list-style-type: none">▪ Erhebliche Konsequenzen▪ Hohe Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none">▪ Personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none">▪ Kann nicht vollständig ausgeschlossen werden
Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none">▪ Schwer und nicht mehr tolerierbar▪ Bedeutende Zielabweichungen
Negative Innen- oder Außenwirkung	<ul style="list-style-type: none">▪ Breite Ansehens- oder Vertrauensbeeinträchtigung
Finanzielle Auswirkungen	<ul style="list-style-type: none">▪ Beträchtlich, jedoch nicht existenzbedrohend

Stufe 4 – SEHR HOCH

Betroffene Datenkategorien	<ul style="list-style-type: none">▪ Personenbezogene Daten gem. Art. 4 Z 1 DSGVO, besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO, wobei die Betroffenen von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existenziell abhängig sind und zusätzliche Risiken bestehen▪ Verschlusssachen
Verstoß gegen Gesetze, Vorschriften und Verträge	<ul style="list-style-type: none">▪ Fundamentale Konsequenzen▪ Ruinöse Konventionalstrafen und Haftungsschäden
Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none">▪ Personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist
Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none">▪ Gravierende Beeinträchtigungen sind möglich▪ Gefahr für Leib und Leben
Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none">▪ Sehr schwer und nicht mehr tolerierbar▪ Existenzielle Zielabweichungen bis hin zur Handlungsunfähigkeit
Negative Innen- oder Außenwirkung	<ul style="list-style-type: none">▪ Landesweite Ansehens- oder Vertrauensbeeinträchtigung
Finanzielle Auswirkungen	<ul style="list-style-type: none">▪ Existenzbedrohend

2.3. Bedarfsanalyse

Die Bedarfsanalyse ist zentraler Bestandteil der strategischen Planung und folgt unmittelbar auf die Schutzbedarfsfeststellung. Wichtige Elemente der Bedarfsanalyse, wie etwa die Berücksichtigung rechtlicher und betrieblicher Rahmenbedingungen, werden im Folgenden skizziert.

2.3.1. Rechtliche Rahmenbedingungen

Auch wenn Geschäftsprozesse an einen Cloud-Service-Provider ausgelagert werden, verbleibt die Verantwortung für die rechtskonforme Abwicklung und somit auch die damit einhergehende Kontrollpflicht beim Cloud-Service-Kunden. Daher gilt es im Rahmen der Bedarfsanalyse genau zu prüfen, welche [Rechtsvorschriften](#) und Pflichten im Einzelfall zutreffen und somit bei der Festlegung von Anforderungen an den Cloud-Service-Provider zu berücksichtigen sind. Nachfolgend sind einige in Österreich relevante Rechtsvorschriften gelistet.

BAO

Die Bundesabgabenordnung regelt u. a. Aufbewahrungsfristen für abgabenrechtliche Daten wie Buchhaltungsdaten, Rechnungen und Belege sowie die Verantwortung für die sichere Aufbewahrung und Wiedergabe der Daten.

BVergG 2006

Das Bundesvergabegesetz 2006 regelt u. a. das Verfahren zur Beschaffung von Leistungen durch öffentliche Auftraggeber, wie z. B. Schwellenwerte, Ausschreibungsbestimmungen, Bekanntmachungen und Fristen.

BVergGVS 2012

Das Bundesvergabegesetz Verteidigung und Sicherheit 2012 regelt u. a. das Verfahren zur Beschaffung von Leistungen durch öffentliche Auftraggeber im Verteidigungs- und Sicherheitsbereich.

DSG 2000

Das Datenschutzgesetz 2000 regelt den Schutz personenbezogener Daten, insb. das Grundrecht auf Datenschutz, die Voraussetzung und Zulässigkeit der Verwendung von Daten, die Pflichten der Auftraggeber und Dienstleister, die erforderlichen Datensicherheitsmaßnahmen, die Geheimhaltungspflicht für Auftraggeber, Dienstleister und ihre Mitarbeiterinnen und Mitarbeiter sowie die Rechte von Betroffenen. Es tritt mit 25. Mai 2018 außer Kraft.

DSG

Das Datenschutzgesetz tritt mit 25. Mai 2018 in Kraft und regelt ergänzende Festlegungen zur Datenschutz-Grundverordnung sowie die Durchführung der Datenschutzrichtlinie, RL (EU) 2016/680 - DSRL-PJ, betreffend die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei, des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs.

DSGVO

Die Datenschutz-Grundverordnung vereinheitlicht die Regelungen für die Verarbeitung von personenbezogenen Daten EU-weit. Sie ist mit 25. Mai 2016 in Kraft getreten und ab 25. Mai 2018 anzuwenden.

E-GovG

Das E-Government-Gesetz regelt die Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen. Dies betrifft u. a. die Schaffung und den Einsatz besonderer technischer Mittel zur Verbesserung des Rechtsschutzes (Sicherheit und Datenschutz) im elektronischen Verkehr sowie die Einhaltung internationaler Standards über die Web-Zugänglichkeit bei der Gestaltung von behördlichen Internetauftritten (Barrierefreiheit).

eIDAS-VO

Die eIDAS-Verordnung regelt u. a. Bedingungen für die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, wie z. B. elektronische Signaturen, elektronische Siegel und elektronische Zeitstempel, die Zustellung elektronischer Einschreiben, die Website-Authentifizierung sowie Validierungs- sowie Bewahrungsdienste.

GTelG 2012

Das Gesundheitstelematikgesetz 2012 regelt Datensicherheitsbestimmungen für den elektronischen Verkehr mit Gesundheitsdaten sowie das Informationsmanagement für Angelegenheiten der Gesundheitstelematik.

GTelV 2013

Die Gesundheitstelematikverordnung 2013 konkretisiert das GTelG 2012 in technischen Fragen zur Datensicherheit. Sie legt u. a. fest, wie die Identität von Gesundheitsdiensteanbietern und die Vertraulichkeit und Integrität von Gesundheitsdaten im Rahmen des elektronischen Gesundheitsdatenaustausches sicherzustellen sind.

InfoSiG

Das Informationssicherheitsgesetz regelt die rechtlichen Grundlagen für die Umsetzung völkerrechtlicher Verpflichtungen Österreichs zur sicheren Verwendung von klassifizierten Informationen, unabhängig von Darstellungsform und Datenträger, im Bereich der Dienststellen des Bundes.

InfoSiV

Die Informationssicherheitsverordnung normiert nähere Bestimmungen zum InfoSiG. Sie regelt u. a. Kennzeichnungs-, Registrierung- und Unterweisungspflichten sowie Maßnahmen und Regeln im Umgang mit klassifizierten Informationen.

NIS-RL

Die EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit definiert Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der europäischen Union und ist mit 8. August 2016 in Kraft getreten.

NISG

Die NIS-RL wird durch das Netz- und Informationssystemssicherheitsgesetz umgesetzt. Das NISG tritt voraussichtlich im Mai 2018 in Kraft und legt Maßnahmen fest, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste in bestimmten Sektoren, Anbietern digitaler Dienste und den verfassungsmäßigen Einrichtungen des Bundes, erreicht werden soll.

SVG

Das Signatur- und Vertrauensdienstegesetz regelt jene Bereiche, in denen die (unmittelbar anwendbare) eIDAS-VO den Mitgliedstaaten die Möglichkeit überlässt, nationale Vorschriften zu erlassen. Dies betrifft insb. Regelungen bzw. Konkretisierungen in den Bereichen der Vertrauensdiensteanbieter, Aufsicht, Formvorschriften, Haftung und Sanktionen.

SVV

Die Signatur- und Vertrauensdiensteverordnung konkretisiert das SVG insb. in technischen Fragen, wie z. B. hinsichtlich der Anforderungen an qualifizierte Vertrauensdiensteanbieter und deren Personal bei der Erbringung qualifizierter Vertrauensdienste sowie der Anforderungen an Vertrauensdiensteanbieter beim Betrieb einer Zertifikatsdatenbank.

TKG 2003

Das Telekommunikationsgesetz 2003 regelt u. a. die Gewährleistung der Sicherheit und Integrität von öffentlichen Kommunikationsnetzen und verpflichtet Betreiber von öffentlichen Kommunikationsnetzen und -diensten angemessene technische und organisatorische Maßnahmen zu ergreifen.

TKG-DSVO

Die Datensicherheitsverordnung normiert u. a. nähere Bestimmungen zur Datensicherheit und Protokollierung bei der Übermittlung von Auskünften über Verkehrsdaten sowie zur Datensicherheit bei der Speicherung und der Zugriffsprotokollierung von Vorratsdaten.

Urheberrechtsgesetz

Das Urheberrechtsgesetz regelt das Urheberrecht im engeren Sinn, das den Schutz von Werken umfasst. Es regelt zudem das Urheberrecht im weiteren Sinn (die sogenannten verwandten Schutzrechte), das den Schutz von bestimmten sonstigen Leistungen umfasst.

Im Rahmen der Bedarfsanalyse sollten bei der Identifizierung der rechtlichen Verpflichtungen insb. folgende Punkte geprüft werden:

- Durchführungspflichten betreffend Risikoanalysen und Folgenabschätzungen
- Umsetzungs-, Prüfungs- und Anpassungspflichten betreffend angemessene Sicherheitsmaßnahmen
- Dokumentations-, Belehrungs- und Unterweisungspflichten
- Kennzeichnungs- und Registrierungspflichten
- Protokollierungs-, Schutz- und Aufbewahrungspflichten
- Auskunft-, Richtigstellungs-, Beschränkungs- und Löschpflichten
- Informationspflichten bei Sicherheitsvorfällen und Datenschutzverletzungen

Je nach Anwendungsdomäne, in der ein Einsatz von Cloud-Services angedacht wird, können auch zusätzliche domänenspezifische Rechtsvorschriften von Bedeutung sein. Beispielsweise besteht im Finanzbereich im Zusammenhang mit Basel III, SOX und EURO-SOX für viele Organisationen die Verpflichtung zur Implementierung eines internen Kontrollsystems (IKS) und eines Risikomanagementsystems (RMS). Entsprechende Vorgaben sind u. a. in folgenden Gesetzen enthalten:

- Aktiengesetz
- Bankwesengesetz
- Genossenschaftsgesetz
- GmbH-Gesetz
- Versicherungsaufsichtsgesetz 2016

Ein weiteres Beispiel, in dem potenziell domänenspezifische rechtliche Anforderungen berücksichtigt werden müssen, ist der Bereich E-Government. Für diese – vor allem für die öffentliche Verwaltung relevante – Domäne existieren in Österreich die österreichischen [E-Government-Konventionen](#), die zahlreiche Empfehlungen und Konzepte zu nachfolgenden Themenbereichen umfassen.

Infrastruktur und Interoperabilität

Architektur, e-Procurement, Zustellung, Bürgerkarte, Cloud Computing, EDIAKT und EDIDOC sowie Langzeitarchivierung

Integration und Zugänge

Portalverbund und LDAP-Verzeichnisdienste

Recht und Sicherheit

Datensicherheitsmaßnahmen für Webanwendungen, Internetpolicy und Amtssignatur

Präsentation und Standarddaten

Styleguide und Standarddaten, Verfahrensvernetzung

Weitere Themen

Big Data, Dienstleistungsrichtlinie, elektronische Einkommensnachweise, E-Democracy, Public Relations und Schulung, E-Government-Anwendungen und Betriebshandbücher sowie Open Government Data

2.3.2. Betriebliche Rahmenbedingungen

Neben rechtlichen Rahmenbedingungen können im Zuge der Bedarfsanalyse auch betriebliche Rahmenbedingungen eine Rolle spielen. Bei deren Erhebung bzw. Festlegung sind organisatorische und technische Bedarfsaspekte im Zusammenhang mit dem Einsatz von Cloud-Services zu klären.

Die nachfolgenden Tabellen stellen eine Auswahl wichtiger Fragen zur Leistungsfähigkeit, Verfügbarkeit, Interoperabilität, zum Zugriffsschutz, Support und zur Flexibilität dar, die im Rahmen der Bedarfsanalyse potenziell geklärt werden müssen. Um die Komplexität gering zu halten, wurde bei den angeführten Aspekten jedoch bewusst nicht zwischen den Service-Modellen unterschieden.

LEISTUNGSFÄHIGKEIT

Anwenderanzahl	<ul style="list-style-type: none">▪ Wie hoch ist die Anzahl der Anwender des Cloud-Services?▪ Gesamtanzahl und Anzahl der gleichzeitigen Anwender▪ interne, externe Anwender
Kapazitätsbedarf	<ul style="list-style-type: none">▪ Welche Kapazitäten muss das Cloud-Service unterstützen?▪ z. B. Datenvolumen, Transaktionen, Anzahl Formulare, Masken, Mailboxgröße, Fileshares etc.
Datenarchivierung	<ul style="list-style-type: none">▪ Ist eine Datenarchivierung erforderlich?
Skalierbarkeit	<ul style="list-style-type: none">▪ Welche Skalierbarkeit muss das Cloud-Service unterstützen?▪ zukünftiger Kapazitätsbedarf
Funktionalitäten	<ul style="list-style-type: none">▪ Welche Prozesse muss das Cloud-Service unterstützen?
Formate	<ul style="list-style-type: none">▪ Welche Formate muss das Cloud-Service unterstützen?▪ Textformate, wie z. B. ASCII, ISO 8859-1, CSV▪ Dokumentenformate, wie z. B. PDF, RTF, Microsoft Office Open XML▪ Grafikformate, wie z. B. GIF, JPEG, TIFF, PNG

- Webformate, wie z. B. HTML 4.0.1, XHTML 1.1, CSS 2
 - Zertifikatsformate, wie z. B. PKCS7, PKCS10, DER, CER, CRL, PEM
 - Komprimierungsformate, wie z. B. ZIP
- Barrierefreiheit
- Bestehen besondere Anforderungen an die Barrierefreiheit des Cloud-Services aufgrund von seh- oder hörbehinderten Anwendern?
- Diakritische Zeichen
- Bestehen besondere Anforderungen an die Unterstützung von diakritischen Zeichen durch das Cloud-Service?

VERFÜGBARKEIT

- Betreute Betriebszeit
- In welchem Zeitraum ist der betreute Betrieb des Cloud-Services jedenfalls sicherzustellen?
 - z. B. Mo. bis Fr., werktags, 08:00 bis 17:00 Uhr
- Serviceverfügbarkeit
- Wie hoch muss die Serviceverfügbarkeit sein?
 - z. B. 99,9 %, 99 %, 98 %, 97 %, 95 %
- Antwortzeiten
- Wie lang dürfen die Antwortzeiten des Cloud-Services maximal sein?
- Planbarkeit
- Wie zeitgerecht müssen Wartungsfenster angekündigt werden?
- Max. tolerierbare Ausfallszeit
- In welchem Zeitraum muss das Cloud-Service nach einem Ausfall wieder zur Verfügung stehen?
- Wiederanlaufzeit
- In welchem Zeitraum muss das Cloud-Service nach einem Ausfall zumindest eingeschränkt wieder zur Verfügung stehen?
 - Notbetrieb
- Wiederanlaufniveau
- Welche Funktionen bzw. Leistungsparameter des Cloud-Services müssen im Notbetrieb zur Verfügung stehen?
- Max. tolerierbarer Datenverlust
- Wie oft müssen die Daten durch das Cloud-Service automatisch gesichert werden?
 - Backup-Frequenz
- Wiederherstellbarkeit
- Wie schnell muss durch das Cloud-Service eine etwaige Datenwiederherstellung durchgeführt werden?
 - Restore

INTEROPERABILITÄT

- Integrationskomplexität
- Wie hoch ist die Integrationskomplexität?
 - bestehende IT-Architektur
- Schnittstellen
- Welche Schnittstellen muss das Cloud-Service unterstützen?
 - z. B. Anbindung an ein internes Identity Management System, Anbindung an weitere Cloud-Services etc.
- Schnittstellenprotokolle
- Welche Schnittstellenprotokolle muss das Cloud-Service unterstützen?
 - z. B. LDAP, Active Directory etc.
- Testmöglichkeiten
- Muss das Cloud-Service vor dem Einsatz getestet werden können?

ZUGRIFFSSCHUTZ

Berechtigungen	<ul style="list-style-type: none">▪ Muss das Cloud-Service unterschiedliche Berechtigungen und Rollen unterstützen?
Authentifizierungsstärke	<ul style="list-style-type: none">▪ Welche Authentifizierungsstärke muss das Cloud-Service unterstützen?▪ Ein-Faktor-Authentifizierung, Zwei-Faktor-Authentifizierung
Authentifizierungsmethoden	<ul style="list-style-type: none">▪ Welche Authentifizierungsmethoden muss das Cloud-Service unterstützen?▪ PIN/Passwort▪ Zertifikats-basierte Methoden▪ One-Time-Passwort▪ SMS-TAN-Verfahren (z. B. Handy-Signatur)▪ biometrische Methoden (Fingerprint-, Iris-Scanner)
Identitätsföderation	<ul style="list-style-type: none">▪ Muss das Cloud-Service Methoden der Identitätsföderation unterstützen?▪ z. B. SAML, WS-Trust, eIDAS Profile etc.
Protokollierung	<ul style="list-style-type: none">▪ Welche Aktivitäten müssen durch das Cloud-Service protokolliert werden?▪ Welche Informationen müssen dabei gespeichert werden?▪ Wie lange müssen die Protokollierungsdaten aufbewahrt werden?

SUPPORT

Online-Hilfe	<ul style="list-style-type: none">▪ Muss das Cloud-Service eine Online-Hilfe zur Verfügung stellen?
Benutzerdokumentation	<ul style="list-style-type: none">▪ Muss das Cloud-Service eine Benutzerdokumentation zur Verfügung stellen?
Benutzerschulung	<ul style="list-style-type: none">▪ Muss das Cloud-Service eine Benutzerschulung zur Verfügung stellen?
Benutzerbetreuung	<ul style="list-style-type: none">▪ Muss das Cloud-Service eine Benutzerbetreuung (Service Desk) zur Verfügung stellen?
Betreuungszeit	<ul style="list-style-type: none">▪ In welchem Zeitraum soll die Benutzerbetreuung verfügbar sein?▪ z. B. Mo. bis Fr., werktags, 08:00 bis 17:00 Uhr
Störungs- und Problemmeldung	<ul style="list-style-type: none">▪ Wer soll Störungen und Probleme im Zusammenhang mit dem Cloud-Service melden dürfen/können?
Störungs- und Problemprozess	<ul style="list-style-type: none">▪ Was soll der Prozess zur Störungs- und Problembeseitigung abdecken?▪ Erreichbarkeit (Telefon, Mail), Sprache (deutsch, englisch)
Reaktionszeit	<ul style="list-style-type: none">▪ Wie schnell muss durch die Benutzerbetreuung reagiert werden?

FLEXIBILITÄT

Agilität	<ul style="list-style-type: none">▪ Wie schnell muss das Cloud-Service einsatzfähig sein?▪ Rollout, Erweiterungen, Provisionierung etc.▪ Pilotbetrieb, Regelbetrieb
Individualisierung	<ul style="list-style-type: none">▪ Muss das Cloud-Service individuell angepasst werden?▪ z. B. Styleguides etc.

2.3.3. Zertifizierungsstandards

Bei der Beurteilung der Konformität von Cloud-Services hinsichtlich der Einhaltung allgemeiner Anforderungen unterstützen neben vertraglichen Vereinbarungen insb. Zertifikate auf Basis von anerkannten Zertifizierungsstandards. Diese Standards sollten im Zuge der Bedarfsanalyse dementsprechend berücksichtigt werden. Die nachfolgende Tabelle stellt eine Auswahl etablierter [Zertifizierungsstandards](#) dar.

ZERTIFIZIERUNGSSTANDARDS	URSPRUNG					
	AT	DE	UK	EU	USA	INT
Business Continuity Management						
ISO 22301						✓
Cloud Computing						
ISO/IEC TR 20000-9						✓
ISO/IEC 27018						✓
Datenschutzmanagement						
BS 10012			✓			
Informationssicherheitsmanagement						
ISO/IEC 27001						✓
ISO/IEC 27001 auf Basis des BSI IT-Grundschutzes		✓				
Rechenzentren						
ANSI/TIA 942					✓	
EN 50600				✓		
Servicemanagement						
ISO/IEC 20000-1						✓
Systemevaluierung						
ISO/IEC 15408						✓
Webapplikationssicherheit						
ÖNORM A-7700	✓					

Tabelle 4: Auswahl etablierter Zertifizierungsstandards

Die Auditierung und Zertifizierung erfolgt durch staatlich akkreditierte Zertifizierungsstellen, die wiederum selbst die Anforderungen von Systemzertifizierungsstandards erfüllen müssen, wie z. B. ISO/IEC 17021, ISO/IEC 20000-6 und ISO/IEC 27006.

2.3.4. Prüfungsstandards

Die Prüfung auf Basis von Prüfungsstandards bietet sich insb. in jenen Fällen an, in denen ein etablierter, aber nicht zertifizierungsfähiger Anforderungskatalog zur Verfügung steht, wie z. B. der BSI Anforderungskatalog (C5) zur Beurteilung der Informationssicherheit von Cloud-Services. Auch hier kann eine Berücksichtigung dieser Prüfungsstandards im Zuge der Bedarfsanalyse hilfreich sein. Die nachfolgende Tabelle stellt eine Auswahl etablierter [Prüfungsstandards](#) dar.

PRÜFUNGSSTANDARDS	URSPRUNG					
	AT	DE	UK	EU	USA	INT
Standard for assurance over non-financial information						
ISAE 3000						✓
Assurance Reports on Controls at a Service Organization						
ISAE 3402						✓
Abschlussprüfung bei Einsatz von Informationstechnologie						
IDW PS 330		✓				
Prüfung von Softwareprodukten						
IDW PS 880		✓				
Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen						
IDW PS 951 n. F.		✓				
Statements on Standards for Attestation Engagements						
AT Section 101					✓	
Reporting on Controls at a Service Organization						
AT Section 801					✓	

Tabelle 5: Auswahl etablierter Prüfungsstandards

Die Prüfung des BSI Anforderungskatalogs (C5) erfolgt beispielsweise auf Grundlage des Prüfungsstandards ISAE 3000 (Revised), der als übergeordneter Prüfungsstandard die allgemeinen Anforderungen an die Qualifikation und das Verhalten einer Prüferin bzw. eines Prüfers und die Annahme, Planung und Durchführung eines Prüfungsauftrags umfasst. Zu besonderen Fragen des Prüfungsvorgehens sowie der Dokumentation und Berichterstattung wird der Prüfungsstandard ISAE 3402 herangezogen.

Ergänzend oder alternativ zu ISAE 3402 können auch der deutsche Prüfungsstandard IDW PS 951 n. F. oder die US-amerikanischen Prüfungsstandards AT Section 801 bzw. AT Section 101 herangezogen werden.

Zu beachten ist, dass die Verfügbarkeit von anerkannten Zertifikaten und Prüfberichten alleine in aller Regel nicht von der Kontrollpflicht befreit, wie z. B. bei der Auftragsverarbeitung von personenbezogenen Daten. Sie stellen aber wichtige Nachweise dar, die die Beurteilung von Cloud-Services wesentlich unterstützen.

2.3.5. Gütesiegel

Zusätzlich zur Zertifizierung und Prüfung von Cloud-Services auf Basis von Zertifizierungs- und Prüfungsstandards bestehen mittlerweile zahlreiche Zertifizierungen auf Basis von Gütesiegeln. Auch diese sollten im Zuge der Bedarfsanalyse geeignet berücksichtigt werden. Die nachfolgende Tabelle stellt eine Auswahl etablierter [Gütesiegel](#) dar.

GÜTESIEGEL	URSPRUNG					
	AT	DE	UK	EU	USA	INT
Datenschutz						
EuroPriSe				✓		
Cloud-Services						
CSA STAR					✓	
ESCloud Label				✓		
EuroCloud StarAudit				✓		
Trusted Cloud-Service		✓				

Tabelle 6: Auswahl etablierter Gütesiegel

2.4. Risikoanalyse

Die Risikoanalyse ist der dritte Schritt im Rahmen der strategischen Planung. Im Rahmen der Risikoanalyse sind die bestehenden Informationssicherheitsrisiken aus Sicht des Cloud-Service-Kunden zu identifizieren und zu analysieren sowie geeignete Sicherheitsmaßnahmen zur Risikoreduzierung festzulegen.

Im Mittelpunkt stehen dabei folgende Schutzziele.



Abbildung 4: Schutzziele der Risikoanalyse

2.4.1. Prozesselemente

Die ISO/IEC Norm 27005 definiert das Informationssicherheitsrisiko als jenes Potenzial, dass eine vorhandene Schwachstelle durch eine Bedrohung ausgenutzt wird und dies zu einem Schaden für die Organisation führt. Der Standard beschreibt den Risikomanagementprozess der systematischen Beurteilung und Behandlung von Informationssicherheitsrisiken.

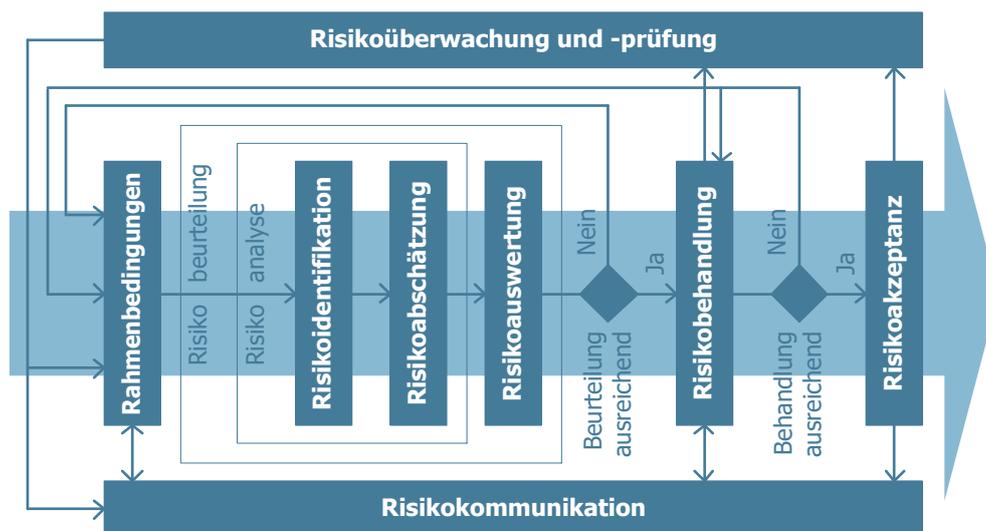


Abbildung 5: Prozesselemente des Risikomanagements

Der Cloud Computing Kompass behandelt nicht den gesamten Risikomanagementprozess, sondern konzentriert sich auf die im Folgenden diskutierten Elemente Risikoidentifikation, Risikoanalyse und -auswertung sowie Risikobewältigung. Weiterführende Informationen zum [Risikomanagement](#) finden sich in den Standards ISO/IEC 27005, ISO/IEC 31000, ONR 49000, im BSI-Standard 100-3 sowie im Österreichischen Informationssicherheitshandbuch.

2.4.2. Risikoidentifikation

Bei der Risikoidentifikation sind alle Organisationswerte (Assets) des Analysebereichs zu erfassen. Dazu zählen die auszulagernden Daten und Datenanwendungen sowie die betroffenen Geschäftsprozesse der Organisation.

Zudem müssen alle relevanten Bedrohungen und vorhandenen Schwachstellen sowie die potenziellen Konsequenzen ermittelt werden, die durch eine Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Datenanwendungen sowie der betroffenen Geschäftsprozesse zu erwarten sind. Hierfür können auch die bei der Schutzbedarfsfeststellung festgelegten Schadensszenarien herangezogen werden.

Um möglichst alle relevanten Bedrohungen zu berücksichtigen, kann deren Identifikation beispielsweise auf Grundlage der Gefährdungskataloge der BSI IT-Grundschutzkataloge erfolgen. Das BSI stellt dafür auch folgende gekürzte Liste von 46 elementaren Gefährdungen aus den Kategorien Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen und Technisches Versagen zur Verfügung.

- Feuer
- Ungünstige klimatische Bedingungen
- Wasser
- Verschmutzung, Staub, Korrosion
- Naturkatastrophen
- Katastrophen im Umfeld
- Großereignisse im Umfeld
- Ausfall oder Störung der Stromversorgung
- Ausfall oder Störung von Kommunikationsnetzen
- Ausfall oder Störung von Versorgungsnetzen
- Ausfall oder Störung von Dienstleistern
- Elektromagnetische Störstrahlung
- Abfangen kompromittierender Strahlung
- Ausspähen von Informationen / Spionage
- Abhören
- Diebstahl von Geräten, Datenträgern und Dokumenten
- Verlust von Geräten, Datenträgern und
- Zerstörung von Geräten oder Datenträgern
- Ausfall von Geräten oder Systemen
- Fehlfunktion von Geräten oder Systemen
- Ressourcenmangel
- Software-Schwachstellen oder -Fehler
- Verstoß gegen Gesetze oder Regelungen
- Unberechtigte Nutzung oder Administration von Geräten und Systemen
- Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- Missbrauch von Berechtigungen
- Personalausfall
- Anschlag
- Nötigung, Erpressung oder Korruption
- Identitätsdiebstahl
- Abstreiten von Handlungen
- Missbrauch personenbezogener Daten
- Schadprogramme
- Verhinderung von Diensten (Denial of Service)

- Dokumenten
- Fehlanpassung oder fehlende Anpassung
- Offenlegung schützenswerter Informationen
- Informationen aus unzuverlässiger Quelle
- Manipulation von Hard- und Software
- Manipulation von Informationen
- Unbefugtes Eindringen in IT-Systeme
- Sabotage
- Social Engineering
- Einspielen von Nachrichten
- Unbefugtes Eindringen in Räumlichkeiten
- Datenverlust
- Integritätsverlust schützenswerter Informationen

2.4.3. Risikoabschätzung und -auswertung

Bei der Risikoabschätzung und -auswertung sind die identifizierten Risiken anhand ihrer Eintrittswahrscheinlichkeit bzw. -häufigkeit und der potenziellen Auswirkungen zu berechnen bzw. einzuschätzen und anhand ihrer Risikohöhe zu priorisieren. Die Ergebnisse dienen als Entscheidungsgrundlage hinsichtlich der Notwendigkeit einer erforderlichen Risikoreduzierung im Rahmen der Risikobewältigung. Die Einschätzung und Priorisierung sollte auf Basis von festgelegten qualitativen oder quantitativen Kriterien und Risikoklassen erfolgen. Die nachfolgende Abbildung zeigt eine beispielhafte Risikomatrix, die für eine Einschätzung und Priorisierung von Risiken verwendet werden kann.

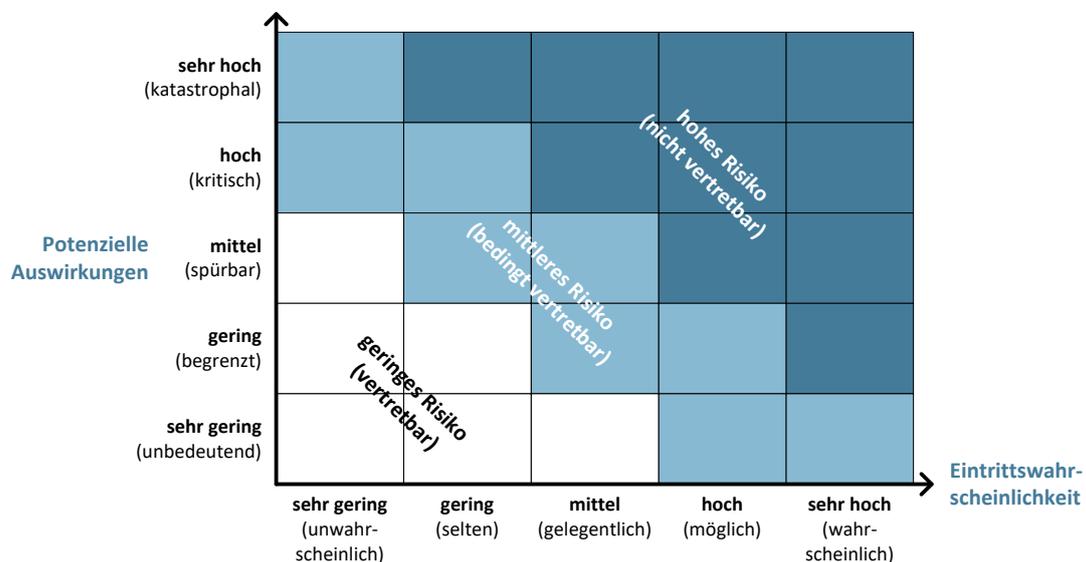


Abbildung 6: Risikomatrixbeispiel mit qualitativen Kriterien

2.4.4. Risikobewältigung

Die Risikobewältigung umfasst die Auswahl und Festlegung geeigneter Maßnahmen zur Veränderung und Steuerung der bewerteten Risiken. Dabei sollten insb. folgende Möglichkeiten geprüft werden.

Risikovermeidung

Entscheidung und Maßnahmen, um eine Risikosituation nicht einzugehen oder sich einer Risikosituation zu entziehen

Risikoverminderung

Entscheidung und Maßnahmen, um die Eintrittswahrscheinlichkeit und/oder die Auswirkungen eines Risikos günstig zu beeinflussen

Risikodiversifikation

Kombination von Tätigkeiten mit unterschiedlichem Risikoprofil, um potenzielle Verluste mit potenziellen Gewinnen auszugleichen

Risikoüberwälzung

Entscheidung und Maßnahmen, um die Auswirkung eines Risikos abzuwälzen, bspw. mittels Auslagerung und Versicherung des Risikos

Risikofinanzierung

Einsatz von Finanzierungsinstrumenten, um die Risiken zu bewältigen und die Liquidität nach Eintritt des Risikos sicherzustellen

Risikotoleranz

Bewusste Entscheidung zur Übernahme eines Risikos im Rahmen der gesetzlichen bzw. regulatorischen Vorgaben

Die nachfolgende Abbildung illustriert die genannten Möglichkeiten der Risikobewältigung und setzt diese miteinander in Beziehung.

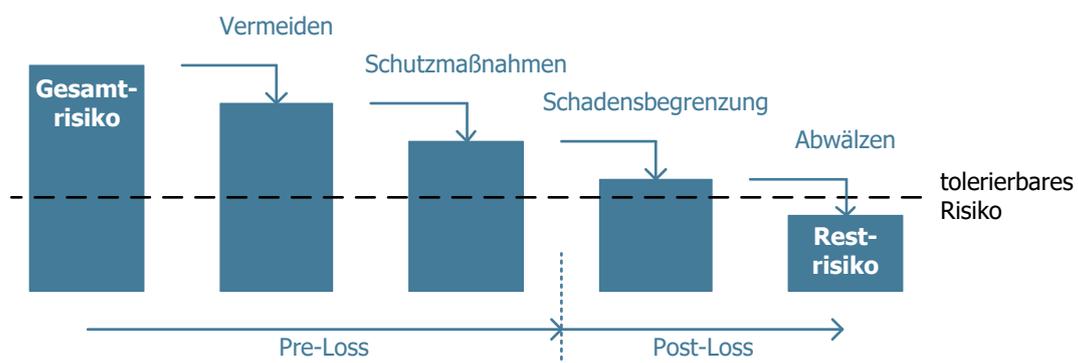


Abbildung 7: Möglichkeiten der Risikobewältigung

Die Risikobewältigung schließt im Allgemeinen mit der Erstellung eines Maßnahmenplans ab, der eine detaillierte Beschreibung der erforderlichen Sicherheitsmaßnahmen enthält.

2.5. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) bildet den letzten Schritt innerhalb der strategischen Planung. Im Rahmen der DSFA sind die bestehenden Datenschutzrisiken aus Sicht der Betroffenen zu identifizieren und zu analysieren sowie geeignete Sicherheitsmaßnahmen zur Risikoreduzierung festzulegen. Im Mittelpunkt stehen dabei folgende Schutzziele.



Abbildung 8: Schutzziele der DSFA

Die im Folgenden skizzierten Elemente einer DSFA beziehen sich zumeist auf die DSGVO. Dieser Fokus wurde bewusst gewählt, da die DSGVO in Zukunft das Fundament datenschutzrechtlicher Aspekte in Europa darstellen wird.

2.5.1. Prozesselemente

Die DSGVO legt primär fest, wann und durch wen eine DSFA durchzuführen ist, was sie zu enthalten hat, wer dabei einzubinden und was zu berücksichtigen ist. Sie lässt weitgehend offen, wie und nach welchen Kriterien eine DSFA durchzuführen ist.

Die DSFA ist kein einmaliger und linearer Prozess, sondern muss erforderlichenfalls mehrmals durchlaufen werden. Der Prozess und die Ergebnisse der DSFA sind ausführlich zu dokumentieren und zu prüfen. Der DSFA-Bericht muss insb. einen Maßnahmenplan mit einer detaillierten Beschreibung der erforderlichen Schutzmaßnahmen enthalten.

Darüber hinaus ist laufend zu überwachen, ob aufgrund von veränderten organisatorischen, technischen oder rechtlichen Rahmenbedingungen hinsichtlich der mit den Verarbeitungsvorgängen verbundenen Risiken Änderungen eingetreten sind. Dies gilt auch für die Wirksamkeit der getroffenen Schutzmaßnahmen.

Der Cloud Computing Kompass behandelt nicht den gesamten Prozess der DSFA, sondern konzentriert sich auf die Relevanzschwelle und die Anforderungen und Kriterien sowie auf die Besonderheiten der DSFA im Vergleich zur Informationssicherheitsrisikoanalyse.

Weiterführende Informationen zur [Datenschutzfolgenabschätzung](#), insb. zum Prozess und zur Berichtsstruktur, finden sich im Standard ISO/IEC 29134.

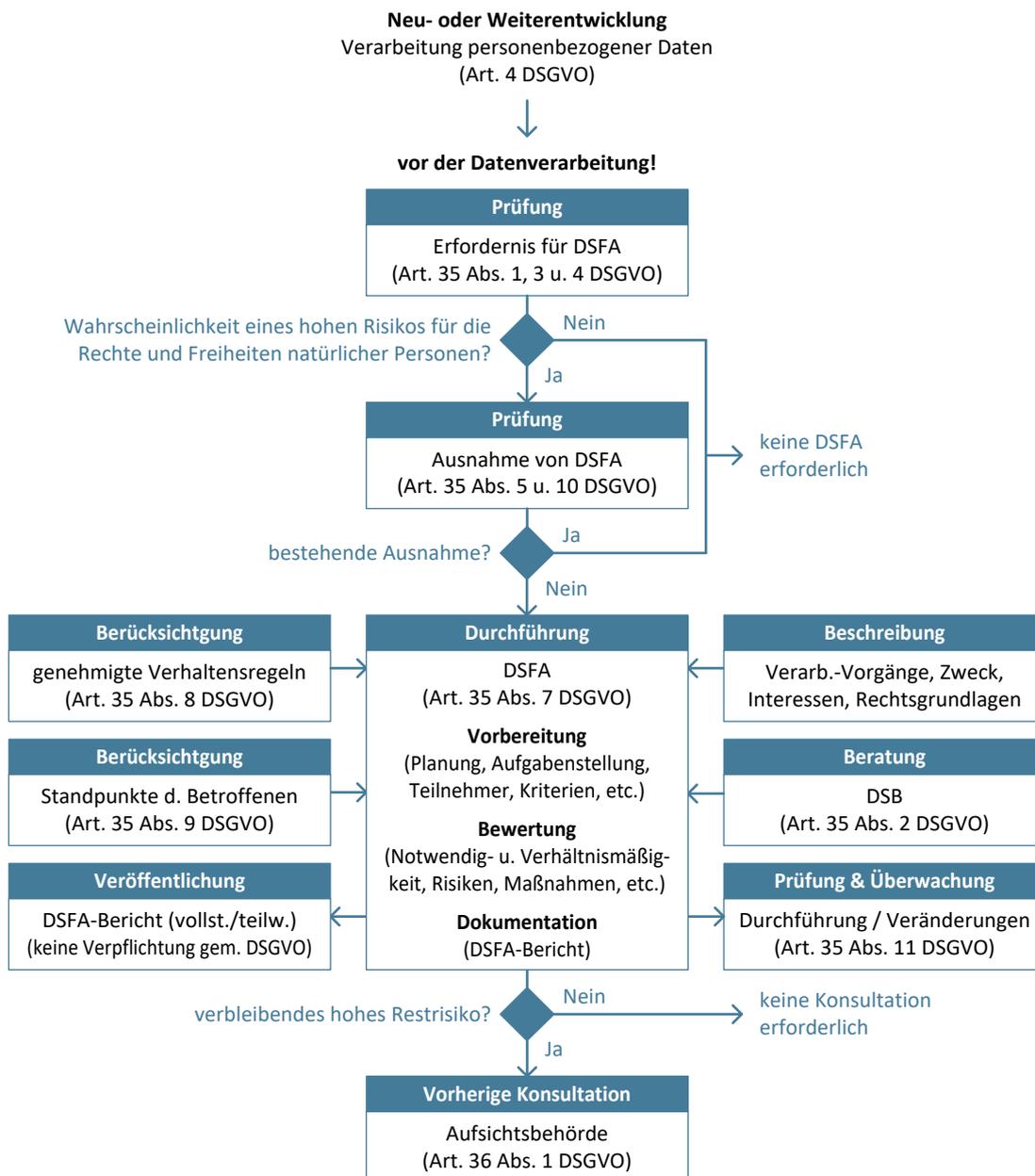


Abbildung 9: Prozesselemente der DSFA

2.5.2. Relevanzschwelle

Gemäß Art. 35 Abs. 1 DSGVO ist eine Datenschutzfolgenabschätzung durchzuführen, wenn die Form der Datenverarbeitung, insb. bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Gemäß Art. 35 Abs. 3 DSGVO ist eine DSFA insb. – jedoch nicht ausschließlich – in den folgenden Fällen erforderlich.

1. Bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschl. Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
2. Bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10.
3. Bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche.

Gemäß Art. 35 Abs. 4 DSGVO hat die Datenschutzbehörde als nationale Aufsichtsbehörde eine Liste jener Verarbeitungsvorgänge zu erstellen und zu veröffentlichen, für die eine DSFA durchzuführen ist. Gemäß Art. 35 Abs. 5 DSGVO kann sie darüber hinaus auch eine Liste jener Verarbeitungsvorgänge erstellen und veröffentlichen, für die keine DSFA erforderlich ist.

Da eine DSFA jedenfalls vor einer etwaigen Datenverarbeitung durchzuführen ist, sind diese Voraussetzungen im Rahmen der Neu- und Weiterentwicklung von Datenanwendungen bereits in der frühen Planungsphase zu prüfen.

2.5.3. Anforderungen

Gemäß Art. 35 Abs. 7 DSGVO muss die DSFA zumindest Folgendes enthalten.

1. Systematische Beschreibung – eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen.

2. Bewertung der Notwendigkeit – eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.

3. Bewertung der Risiken – eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen.

4. Geplante Maßnahmen – die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschl. Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DSGVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Weiterführende Informationen finden sich in den ➔ [Datenschutzrechtliche Orientierungshilfen](#), insb. in der WP29-Richtlinie zur DSFA.

2.5.4. Besonderheiten

Im Vergleich zur Informationssicherheitsrisikoanalyse bestehen bei der Durchführung einer DSFA zwei wesentliche Besonderheiten. Das sind einerseits die Perspektive, aus der die Risikoidentifikation, Risikoanalyse und -auswertung durchzuführen sind, und andererseits die Berücksichtigung von erweiterten Schutzziele.

Bei einer Informationssicherheitsrisikoanalyse erfolgt die Risikobetrachtung aus der Perspektive der Organisation, bei der die Sicherung ihrer Geschäftsprozesse im Vordergrund steht. Bei der DSFA muss dagegen konsequent die Perspektive der Betroffenen eingenommen und der Fokus auf ihre Interessen und Rechte gelegt werden. Auch vom Datenschutzbeauftragten einer Organisation ist zu erwarten, dass er seine Organisation sozusagen von außen betrachtet. Ein gewisser Interessenkonflikt ist dabei naheliegend. Deshalb ist bei der DSFA ein erweitertes Verständnis gefordert, das die Perspektive der Betroffenen geeignet berücksichtigt.

Neben den typischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, die im Rahmen der Informationssicherheitsrisikoanalyse betrachtet werden, sind bei der DSFA zudem die Schutzziele

Transparenz, Nichtverkettung und Intervenierbarkeit zu berücksichtigen. Darüber hinaus werden in diversen datenschutzrechtlichen Leitlinien auch die Aspekte Authentizität, Revisionsfähigkeit und Datenminimierung als Schutzziele genannt. Insgesamt sollten im Zuge einer DSFA daher folgende Schutzziele berücksichtigt werden:

Vertraulichkeit

Vertraulichkeit bezeichnet die Anforderung, dass Unbefugte Daten nicht zur Kenntnis nehmen können. Unbefugte sind nicht nur Dritte außerhalb der Organisation, sondern auch Mitarbeiterinnen und Mitarbeiter von Dienstleistern, die für die Erbringung der Dienstleistung keinen Zugriff auf die Daten benötigen, oder Personen interner Organisationseinheiten, die keinen inhaltlichen Bezug zum Verfahren oder zum Betroffenen haben.

Verfügbarkeit

Verfügbarkeit bezeichnet die Anforderung, dass Daten zur Verfügung stehen müssen und ordnungsgemäß verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Verarbeitungsmethoden müssen auf sie angewendet werden können.

Nichtverkettbarkeit

Nichtverkettung bezeichnet die Anforderung, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden.

Revisionsfähigkeit

Revisionsfähigkeit bezeichnet die Anforderung, dass festgestellt werden kann, wer wann welche Daten in welcher Weise verarbeitet hat. Dazu zählen insb. Zugriffe, Änderungen und Übermittlungen.

Integrität

Integrität bezeichnet einerseits die Eigenschaft, dass die zu verarbeitenden Daten unversehr, vollständig und aktuell bleiben. Integrität bezeichnet andererseits die Anforderung, dass Informationssysteme und -prozesse im Zusammenhang mit den festgelegten und zweckbestimmten Funktionen ordnungsgemäß bleiben.

Transparenz

Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch Verantwortliche, Auftragsverarbeiter sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck erhoben und verarbeitet werden, wohin die Daten zu welchem Zweck übermittelt werden, welche Informationssysteme und -prozesse dafür genutzt werden und wer die rechtliche Verantwortung trägt.

Intervenierbarkeit

Intervenierbarkeit bezeichnet die Anforderung, dass Betroffenen die Ausübung ihrer Rechte auf Information, Auskunft, Berichtigung, Einschränkung, Löschung und Benachrichtigung jederzeit wirksam gewährt wird.

Authentizität

Authentizität bezeichnet die Anforderung, dass Daten ihrem Ursprung gesichert zugeordnet werden können.

Datenminimierung

Datenminimierung konkretisiert und operationalisiert den Grundsatz, nicht mehr Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Zwecks erforderlich ist.

2.5.5. Kriterien

Eine DSGVO-konforme DSFA muss eine Reihe von Anforderungen erfüllen. Die WP29-Richtlinie zur DSFA definiert u. a. nachfolgende Kriterien zur Überprüfung, ob eine DSFA die Anforderungen der DSGVO erfüllt.

KRITERIEN

- | | |
|---|--|
| <p>Liegt eine systematische Beschreibung der Verarbeitungsvorgänge vor.
(Art. 35 Abs. 7 lit. a DSGVO)</p> | <ul style="list-style-type: none">▪ Wesen, Anwendungsbereich, Zusammenhänge und Zwecke wurden berücksichtigt (Erwägungsgrund 90).▪ Art und Umfang der verarbeiteten personenbezogenen Daten, Empfänger und Speicherfristen sind dokumentiert.▪ Eine funktionale Beschreibung der Verarbeitungsvorgänge liegt vor.▪ Alle Systeme für die Datenverarbeitung (Hardware, Software, Netzwerke, Personen, Übertragungskanäle) sind identifiziert.▪ Die Einhaltung genehmigter Verhaltensregeln (Art. 35 Abs. 8 DSGVO) wurde berücksichtigt. |
| <p>Die Notwendigkeit und Verhältnismäßigkeit wurde bewertet.
(Art. 35 Abs. 7 lit. b DSGVO)</p> | <ul style="list-style-type: none">▪ Alle geplanten Schutzmaßnahmen zur Einhaltung der DSGVO wurden festgelegt (Art. 35 Abs. 7 lit. d DSGVO).<ul style="list-style-type: none">▪ Die Schutzmaßnahmen stehen im Einklang mit der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung:<ul style="list-style-type: none">▪ Festgelegter, eindeutiger und legitimer Zwecke (Art. 5 Abs. 1 lit. b DSGVO)▪ Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)▪ Angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt (Art. 5 Abs. 1 lit. c DSGVO)▪ Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)▪ Die Schutzmaßnahmen stehen im Einklang mit den Rechten der Betroffenen:<ul style="list-style-type: none">▪ Transparente Information und Informationspflichten (Art. 12, 13 u. 14 DSGVO)▪ Recht auf Auskunft und Datenübertragbarkeit (Art. 15 u. 20 DSGVO)▪ Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie Widerspruchsrecht (Art. 16 bis 19 u. 21 DSGVO)▪ Empfänger |

- Auftragsverarbeiter (Art. 28 DSGVO)
- Garantien und Sicherheitsvorkehrungen i. Z. m. Übermittlungen an Drittländer oder internationale Organisationen (Kap. V DSGVO)
- Vorherige Konsultation der Aufsichtsbehörde (Art. 36 DSGVO)

Die Risiken für die Rechte und Freiheiten der Betroffenen sind gemanagt.
(Art. 35 Abs. 7 lit. c DSGVO)

- Ursache, Art, Besonderheit und Schwere der Risiken wurden evaluiert oder für jedes Risiko (Vertraulichkeits-, Integritäts- und Verfügbarkeitsverletzungen) aus Sicht der Betroffenen wurden
 - Risikoursachen berücksichtigt
 - Potenzielle Auswirkungen von Vertraulichkeits-, Integritäts- und Verfügbarkeitsverletzungen auf die Rechte und Freiheiten der Betroffenen identifiziert
 - Bedrohungen, die zu Vertraulichkeits-, Integritäts- und Verfügbarkeitsverletzungen führen können, identifiziert
 - Eintrittswahrscheinlichkeit und Schwere bewertet
- Die geplanten Abhilfemaßnahmen zur Bewältigung der Risiken wurden festgelegt (Art. 35 Abs. 7 lit. d DSGVO).

Die interessierten Beteiligten sind involviert.

- Der Rat des DSB wurde eingeholt (Art. 35 Abs. 2 DSGVO).
- Der Standpunkt der Betroffenen oder ihrer Vertreter wurde eingeholt (Art. 35 Abs. 9 DSGVO).

2.6. Fazit

Trotz der zahlreichen Vorteile von Cloud Computing im Vergleich zum klassischen In-House-Betrieb von IT-Infrastruktur muss dessen Einsatz im Rahmen einer strategischen Planung wohlüberlegt und für jeden Anwendungsfall getrennt betrachtet werden. Da für eine solche Betrachtung zahlreiche Aspekte berücksichtigt werden müssen, ist ein systematisches Vorgehen unumgänglich. Eine geeignete strategische Planung muss daher unter anderem eine Schutzbedarfsfeststellung, eine Bedarfsanalyse, eine Risikoanalyse und gegebenenfalls auch eine Datenschutzfolgeabschätzung umfassen.

Zentrale Elemente all dieser Schritte wurden in diesem Abschnitt skizziert. Resultat der durchgeführten strategischen Planung ist eine Entscheidung, ob Cloud Computing für den jeweils gegebenen Anwendungsfall eine mögliche und sinnvolle Alternative ist. Fällt diese Entscheidung positiv aus, müssen im nächsten Schritt ein geeigneter Cloud-Service-Provider gewählt und Anforderungen an diesen definiert werden. Der nachfolgende Abschnitt widmet sich wichtigen Aspekten, die bei diesen Tätigkeiten berücksichtigt werden müssen.

3. Anforderungsspezifikation

Wurde eine Entscheidung für die Verwendung von Cloud-Services getroffen, hängt deren erfolgreicher Einsatz wesentlich von der Qualität der Anforderungen ab, deren Erfüllung zwischen Cloud-Service-Kunden und Cloud-Service-Providern vertraglich vereinbart wurde. Um eine entsprechende Angemessenheit bei der Spezifikation der Anforderungskriterien und der späteren Vertragsgestaltung sicherzustellen, sollten diese auf den gewonnenen Ergebnissen der strategischen Planung aufbauen. Die zu definierenden Anforderungen müssen ein breites Spektrum unterschiedlicher Aspekte berücksichtigen.

Dabei besteht die Gefahr, relevante Aspekte zu übersehen. Um dem entgegenzusteuern, zeigt dieser Abschnitt anhand repräsentativer Anforderungskriterien, welche Aspekte im Zuge der Anforderungsspezifikation beachtet werden müssen. Da Anforderungskriterien nur beispielhaft skizziert werden, erheben diese keinen Anspruch auf Vollständigkeit. Dementsprechend stellt dieser Abschnitt des Cloud Computing Kompasses keinen abschließenden Kriterienkatalog dar.

3.1. Anforderungskriterien

Vertragliche Vereinbarungen zwischen Cloud-Service-Kunden und Cloud-Service-Providern müssen alle wesentlichen Festlegungen hinsichtlich Transparenz, Verbindlichkeit, Nutzung und Bereitstellung von Cloud-Services enthalten. Die im Cloud Computing Kompass abgebildeten Anforderungskriterien unterteilen sich in drei Ebenen mit unterschiedlichen Detailgraden sowie in die drei Säulen Service, Sicherheit und Datenschutz, wobei Letztere nur im Fall einer Verarbeitung von personenbezogenen Daten relevant ist.

Zur Sicherstellung des aktuellen Stands der Technik in den vertraglichen Vereinbarungen sollte insb. bei der Festlegung von technischen Anforderungen und Ausprägungen – soweit und wo dies möglich ist – auf Empfehlungen und Richtlinien etablierter Organisationen referenziert werden, zumal diese üblicherweise einem kontinuierlichen Aktualisierungsprozess unterliegen.

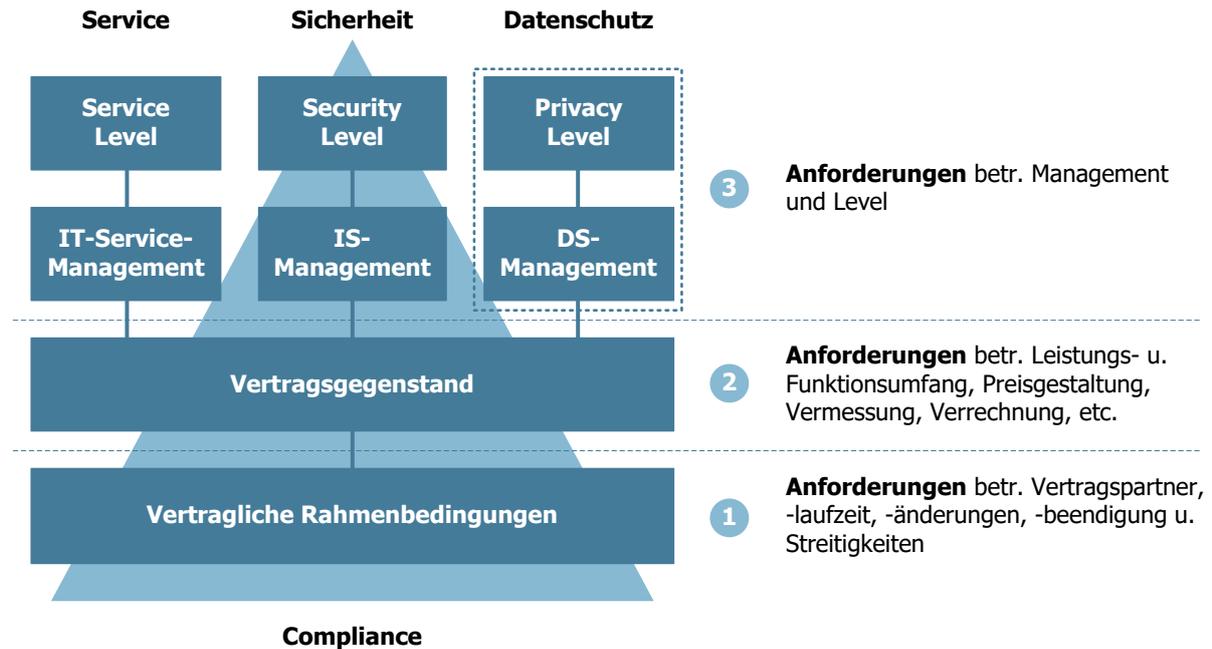


Abbildung 10: Ebenen und Säulen der Anforderungskriterien

Für alle im Cloud Computing Kompass abgebildeten Anforderungen sind jeweils die folgenden Aspekte speziell ausgeführt.

1. Schutzbedarf – beschreibt bei welchem Schutzbedarf die Anforderung in die vertraglichen Vereinbarungen aufgenommen werden sollte.

2. Anforderung – enthält die Beschreibung der Anforderung für die vertraglichen Vereinbarungen zwischen Cloud-Service-Kunden und Cloud-Service-Provider.

3. Referenzierte Standards (optional) – enthält etwaige referenzierte Empfehlungen und Richtlinien etablierter Organisationen hinsichtlich der konkreten Anforderungen oder Ausprägungen.

4. Weiterführende Informationen (optional) – enthält Verweise auf Leitfäden, Rechtsvorschriften, Konventionen, Standards oder Normen mit weiterführenden Informationen.

Der Schutzbedarf ergibt sich aus einer Kombination der einzelnen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit). Die vorgenommene Zuordnung relevanter Schutzbedarfskategorien zu den einzelnen Anforderungen ist indikativ zu verstehen. Je nach konkretem Anwendungsfall kann es in der Realität notwendig sein, hier Adaptierungen vorzunehmen.

3.2. Vertragliche Rahmenbedingungen

Folgende Rahmenbedingungen sind vor Vortragsabschluss zwischen Cloud-Service-Provider und Cloud-Service-Kunden festzulegen.

3.2.1. Vertragspartner

3.2.1.1. Cloud-Service-Provider

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über alle an der Erbringung des Vertragsgegenstands beteiligten Dienstleister und Subdienstleister zur Verfügung.</p> <p>Dazu zählen insb. Firmenname, Anschrift, Internetadresse der Homepage, Rechtsform, Beteiligungsverhältnisse, Unternehmenszentrale, weitere Niederlassungen, Umsatzsteueridentifikationsnummer, Firmenbuch-, Gewerbe- oder Vereinsregistereintragungen, Unternehmensprofil sowie Angaben über Anzahl der Mitarbeiterinnen und Mitarbeiter, Umsatz, Unternehmenskategorie, Anzahl der Cloud-Services und Erfahrung mit der Bereitstellung von Cloud-Services.</p>			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.1.2. Standorte

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider gibt dem Cloud-Service-Kunden sämtliche Standorte bekannt, die zur Erbringung des Vertragsgegenstands genutzt werden, einschl. Standorte weiterer Dienstleister und Subdienstleister. Dies gilt insb. für das Hosting von Systemen sowie für die Verarbeitung, Speicherung und Sicherung von Daten.</p>			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.1.3. Kontaktdaten

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden die Kontaktdaten der Ansprechpartner hinsichtlich Vertrieb, Service, Informationssicherheit, Datenschutz, Support, Verrechnung und Recht zur Verfügung. Dazu zählen insb. Name, Telefonnummer und E-Mail-Adresse.			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.1.4. Geschäftsbedingungen

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden alle allgemeinen Geschäftsbedingungen, die im Zusammenhang mit der Erbringung des Vertragsgegenstands relevant sind, zur Verfügung.			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.1.5. Anwendbares Recht und Gerichtsstand

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider gibt dem Cloud-Service-Kunden das anwendbare Recht und den Gerichtsstand im Zusammenhang mit der Erbringung des Vertragsgegenstands bekannt.			
Anmerkungen			
Empfohlen wird österreichisches Recht unter Ausschluss der Verweisungsnormen sowie ein österreichischer Gerichtsstand.			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.1.6. Offenbarungs- und Ermittlungsbefugnisse

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider verpflichtet sich, den Cloud-Service-Kunden schriftlich über etwaige Offenbarungspflichten bzw. Ermittlungs- und Eingriffsbefugnisse von Gerichten, Strafverfolgungsbehörden und Geheimdiensten sowie über Einsichtsrechte Dritter zu informieren, die einen Zugriff auf Daten und Datenanwendungen des Cloud-Service-Kunden ermöglichen könnten. Dies gilt auch für alle an der Erbringung des Vertragsgegenstands beteiligten weiteren Dienstleister und Subdienstleister.			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.1.7. Unvereinbarkeit von Vertragsverpflichtungen

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider garantiert, dass er keinen Rechtsvorschriften oder vertraglichen Vereinbarungen unterliegt, die ihm die Erfüllung seiner Vertragsverpflichtungen mit dem Cloud-Service-Kunden unmöglich machen und dass er im Fall einer Änderung von Rechtsvorschriften oder vertraglichen Vereinbarungen, die sich voraussichtlich nachteilig auf die Erfüllung seiner Vertragsverpflichtungen mit dem Cloud-Service-Kunden auswirken, den Cloud-Service-Kunden hiervon umgehend informieren wird. Der Cloud-Service-Provider garantiert dies auch für alle an der Erbringung des Vertragsgegenstands beteiligten weiteren Dienstleister und Subdienstleister.			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.2. Vertragslaufzeit und -änderungen

3.2.2.1. Vertragslaufzeit und -verlängerung

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über Regelungen zur Vertragslaufzeit und zur Vertragsverlängerung zur Verfügung, einschl. etwaiger Fristen.			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Cloud-Grundlagen➔ Cloud-Strategie			

3.2.2.2. Änderungen von Vertragsbedingungen

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider garantiert, dass Änderungen von Vertragsbedingungen ausschließlich schriftlich erfolgen und eine einseitige Änderung ausgeschlossen ist.			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Cloud-Grundlagen ➔ Cloud-Strategie 			

3.2.2.3. Hinzuziehung weiterer Dienstleister und Subdienstleister

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider garantiert, dass bei der Erbringung des Vertragsgegenstands eine Hinzuziehung weiterer Dienstleister und Subdienstleister bzw. Ersetzung durch andere Dienstleister und Subdienstleister nur mit Billigung und nach schriftlicher Zustimmung des Cloud-Service-Kunden erfolgt und er den Cloud-Service-Kunden von einer beabsichtigten Hinzuziehung oder Ersetzung so rechtzeitig verständigt, dass dieser dies allenfalls untersagen kann.</p> <p>Der Cloud-Service-Provider stellt zudem sicher, dass diese Dienstleister und Subdienstleister hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Erbringung des Vertragsgegenstands im Einklang mit den gegenständlichen vertraglichen Vereinbarungen und den geltenden rechtlichen Bestimmungen erfolgt.</p>			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Rechtsvorschriften ➔ Datenschutzrechtliche Orientierungshilfen 			

3.2.2.4. Hinzuziehung weiterer Standorte

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider garantiert, dass bei der Erbringung des Vertragsgegenstands eine Hinzuziehung weiterer Standorte bzw. Ersetzung durch Standorte in anderen als den festgelegten Ländern nur mit Billigung und nach schriftlicher Zustimmung des Cloud-Service-Kunden erfolgt und er den Cloud-Service-Kunden von einer beabsichtigten Hinzuziehung oder Ersetzung so rechtzeitig verständigt, dass dieser dies allenfalls untersagen kann. Dies gilt auch für Standorte aller an der Erbringung des Vertragsgegenstands beteiligten weiteren Dienstleister und Subdienstleister.			
Anmerkungen			

Siehe datenschutzrechtliche Vorschriften (insb. Datenübermittlung an Drittländer und internationale Organisationen).

Weiterführende Informationen

- ➔ Rechtsvorschriften
- ➔ Datenschutzrechtliche Orientierungshilfen

3.2.2.5. Preisanpassungen

Schutzbedarf

<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
--	--	--	---

Anforderung

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über Regelungen hinsichtlich etwaiger Preisanpassungen zur Verfügung.

Weiterführende Informationen

- ➔ Cloud-Grundlagen
- ➔ Cloud-Strategie

3.2.3. Vertragsbeendigung und -streitigkeiten

3.2.3.1. Vertragsbeendigung

Schutzbedarf

<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
--	--	--	---

Anforderung

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über Regelungen zur Vertragsbeendigung zur Verfügung. Dazu zählen insb. Kündigungsgründe, Prozesse, Fristen und Kosten der Rückgabe, Aufbewahrung oder Vernichtung von Daten des Cloud-Service-Kunden samt zugehöriger Passwörter, Schlüssel und dgl.

Weiterführende Informationen

- ➔ Cloud-Grundlagen
- ➔ Cloud-Strategie

3.2.3.2. Datenrückgabe, -aufbewahrung und -vernichtung

Schutzbedarf

<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
--	--	--	---

Anforderung

Der Cloud-Service-Provider garantiert, dass er nach Vertragsbeendigung sämtliche Daten des Cloud-Service-Kunden sowie sämtliche Verarbeitungsergebnisse und Unterlagen, die Daten des Cloud-Service-Kunden enthalten, dem Cloud-Service-Kunden übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufbewahren oder auftragsgemäß löschen bzw. vernichten wird.

Die Löschung bzw. Vernichtung hat unter Einhaltung etablierter Sicherheitsstandards zu erfolgen.

Referenzierte Standards

- ISO/IEC 27040
- SP 800-88

Weiterführende Informationen

- ➔ Rechtsvorschriften
- ➔ Datenschutzrechtliche Orientierungshilfen
- ➔ Datenlöschung

3.2.3.3. Insolvenz

Schutzbedarf

- | | | | |
|--|--|--|---|
| <input checked="" type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|--|--|--|---|

Anforderung

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über Regelungen bei einer etwaigen Insolvenz des Cloud-Service-Providers zur Verfügung. Dazu zählen insb. vorbeugende Maßnahmen hinsichtlich der Sicherstellung des Betriebs und der Bereitstellung der Daten sowie geltendes Insolvenzrecht und etwaige Treuhänderregelungen.

Weiterführende Informationen

- ➔ Cloud-Grundlagen
- ➔ Cloud-Strategie

3.2.3.4. Streitigkeiten

Schutzbedarf

- | | | | |
|--|--|--|---|
| <input checked="" type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|--|--|--|---|

Anforderung

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über Regelungen bei etwaigen Streitigkeiten im Rahmen der Erbringung des Vertragsgegenstands zur Verfügung. Dazu zählen insb. Streitigkeiten über die Leistungserbringung, Leistungsmessung, Leistungsverrechnung und Zahlungsverzug.

Weiterführende Informationen

- ➔ Cloud-Grundlagen
- ➔ Cloud-Strategie

3.3. Vertragsgegenstand

3.3.1. Allgemeine Vereinbarungen

3.3.1.1. Leistungs- und Funktionsumfang

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über den zugesicherten Leistungs- und Funktionsumfang des Cloud-Services zur Verfügung. Dazu zählen insb. Leistungs-, Performance- und Kapazitätsdaten, Funktionsbeschreibungen, Bereitstellungs- und Servicemodell und etwaige BBG-Abrufbarkeit.			
Weiterführende Informationen			
→ Cloud-Grundlagen → Cloud-Strategie			

3.3.1.2. Benutzer-Support

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über den zugesicherten Benutzer-Support zur Verfügung. Dazu zählen insb. garantierte Supportleistungen, Betreuungszeitraum, verfügbare Kommunikationskanäle und Sprachen, garantierte Verfügbarkeiten und Reaktionszeiten, verwendetes Ticketsystem sowie verfügbare Online-Hilfen, Benutzerdokumentation und Benutzerschulungen.			
Weiterführende Informationen			
→ Cloud-Grundlagen → Cloud-Strategie			

3.3.1.3. Reifegrad und Referenzen

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über den Reifegrad des Cloud-Services zur Verfügung. Dazu zählen Kennzahlen wie Anzahl der Kunden und Gesamtnutzer, aktuelle Versionsnummer und aktuelles Versionsdatum sowie Name, Land und Branche von Referenzkunden und Name, Telefonnummer und E-Mail-Adresse einer Ansprechpartnerin bzw. eines Ansprechpartners.			
Weiterführende Informationen			
→ Cloud-Grundlagen			

→ Cloud-Strategie

3.3.1.4. Implementierungs- und Nutzungsvoraussetzungen

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die organisatorischen und technischen Voraussetzungen zur Implementierung und Nutzung des Cloud-Services zur Verfügung.</p> <p>Dazu zählen insb. Interoperabilität mit anderen Cloud-Services, Benutzer- und Rechteverwaltung und Anbindungsmöglichkeiten an externe ID-Managementsysteme, Administrations- und Provisionierungsprozesse und -regelungen und Authentifizierungsmethoden, Schnittstellenprotokolle und -formate, Umgebungsbedingungen, Systemvoraussetzungen, Sprachversionen, Customizing-Möglichkeiten, Abnahmeprozesse sowie separat zu verrechnende Sonderleistungen.</p>			
Weiterführende Informationen			
<p>→ Cloud-Grundlagen</p> <p>→ Cloud-Strategie</p>			

3.3.1.5. Testmöglichkeiten

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über etwaige Möglichkeiten zum Test des Cloud-Services in der Vorvertragsphase zur Verfügung. Dazu zählen insb. etwaige Leistungs-, Performance-, Kapazitäts- und Funktionseinschränkungen sowie zu verrechnende Kosten.</p>			
Weiterführende Informationen			
<p>→ Cloud-Grundlagen</p> <p>→ Cloud-Strategie</p>			

3.3.1.6. Preisgestaltung, Leistungsmessung und -verrechnung

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über Preisgestaltung, Leistungsmessung und Leistungsverrechnung des Cloud-Services zur Verfügung. Dazu zählen insb. Upgrade- und Downgrade-Möglichkeiten, separat zu verrechnende Sonderleistungen, Mengenrabatte sowie Entgeltminderungen, Pönalen und Schadenersatz bei Leistungsstörungen.</p>			

Weiterführende Informationen

- Cloud-Grundlagen
- Cloud-Strategie

3.3.1.7. Mitwirkungspflichten

Schutzbedarf

- | | | | |
|--|--|--|---|
| <input checked="" type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|--|--|--|---|

Anforderung

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die Mitwirkungspflichten des Cloud-Service-Kunden im Zusammenhang mit der Erbringung des Vertragsgegenstands zur Verfügung.

Weiterführende Informationen

- Cloud-Grundlagen
- Cloud-Strategie

3.3.1.8. Dokumentationsanforderungen

Schutzbedarf

- | | | | |
|--|--|--|---|
| <input checked="" type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|--|--|--|---|

Anforderung

Der Cloud-Service-Provider stellt sicher, dass die bereitgestellte schriftliche Dokumentation hinsichtlich der vertraglichen Rahmenbedingungen und des Vertragsgegenstands ausreichende, nachvollziehbare und transparente Angaben enthält, die es einem sachverständigen Dritten erlauben, die Eignung des Cloud-Service-Providers und des Cloud-Services sowie die Angemessenheit und Wirksamkeit der beschriebenen Angaben und Garantien zu beurteilen.

Weiterführende Informationen

- Cloud-Grundlagen
- Cloud-Strategie

3.3.1.9. Auftragsgemäße Datenverarbeitung

Schutzbedarf

- | | | | |
|--|--|--|---|
| <input checked="" type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|--|--|--|---|

Anforderung

Der Cloud-Service-Provider garantiert, dass die Verarbeitung von Daten des Cloud-Service-Kunden ausschließlich im Rahmen seines Auftrags und ausschließlich in Produktivumgebungen erfolgt und eine Verwendung der Daten für andere Zwecke oder für Zwecke Dritter sowie die Weitergabe oder Übermittlung an Dritte unterbleiben. Der Cloud-Service-Provider garantiert darüber hinaus, dass eine Verarbeitung von Daten des Cloud-Service-Kunden in anderen Systemumgebungen, wie z. B. Entwicklung- oder Testumgebungen, unterbleibt.

Weiterführende Informationen

- ➔ Rechtsvorschriften
- ➔ Datenschutzrechtliche Orientierungshilfen

3.3.1.10. Geheimhaltungspflichten

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verpflichtet sich, alle erlangten Kenntnisse über schutzwürdige Geheimhaltungsinteressen des Cloud-Service-Kunden geheim zu halten und für einen entsprechenden Schutz dieser Informationen zu sorgen. Diese Verpflichtung besteht bereits in der Phase der Vertragsanbahnung sowie im Rahmen der Vertragserfüllung und nach Vertragsbeendigung. Diese Geheimhaltungspflicht gilt auch für alle an der Erbringung des Vertragsgegenstands beteiligten weiteren Dienstleister und Subdienstleister.</p> <p>Als schutzwürdige Geheimhaltungsinteressen gelten organisationsinterne Informationen, die nicht zur Veröffentlichung bestimmt sind sowie Informationen, die gesetzlichen Geheimhaltungspflichten unterliegen, insb. Amts-, Berufs-, Geschäfts- und Betriebsgeheimnisse gem. StGB. Der Cloud-Service-Provider verpflichtet sich, diese Geheimhaltungspflichten an alle an der Erbringung des Vertragsgegenstands beteiligten weiteren Dienstleister und Subdienstleister zu überbinden.</p>			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Rechtsvorschriften ➔ Datenschutzrechtliche Orientierungshilfen 			

3.3.1.11. Belehrungspflichten

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verpflichtet sich, alle an der Erbringung des Vertragsgegenstands beteiligten Personen vor der Aufnahme ihrer Tätigkeit schriftlich zur Einhaltung der bestehenden Geheimhaltungspflichten zu belehren. Diese Belehrungspflicht gilt auch für alle an der Erbringung des Vertragsgegenstands beteiligten weiteren Dienstleister und Subdienstleister.</p>			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Rechtsvorschriften ➔ Datenschutzrechtliche Orientierungshilfen 			

3.3.1.12. Sicherheitsüberprüfung von Personen

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider verpflichtet sich bei Vorliegen besonderer Vertraulichkeitsanforderungen, wie z. B. bei der Verarbeitung von klassifizierten Informationen gem. InfoSiG oder GehSO, ausschließlich Personen einzusetzen, die im Umgang mit klassifizierten Informationen gem. InfoSiV nachweislich unterwiesen wurden und deren Verlässlichkeit durch eine Sicherheitsüberprüfung gem. §§ 55 ff SPG überprüft wurde. Dies gilt auch für etwaige weitere Dienstleister und Subdienstleister.			
Weiterführende Informationen			
➔ Rechtsvorschriften			

3.3.1.13. Pönale bei Verletzung von Vertragspflichten

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider verpflichtet sich im Fall einer Verletzung seiner Vertragspflichten zur Zahlung eines Pönales.			
Weiterführende Informationen			
➔ Cloud-Grundlagen			
➔ Cloud-Strategie			

3.3.1.14. Freistellung des Cloud-Service-Kunden von Ansprüchen Dritter

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Der Cloud-Service-Provider garantiert, dass er über alle für die Erbringung des Vertragsgegenstands erforderlichen Nutzungsrechte verfügt und den Cloud-Service-Kunden von etwaigen Ansprüchen Dritter, insb. wegen einer Verletzung von Urheber- und Patentrechten oder sonstigen Schutzrechten, freistellt.			
Weiterführende Informationen			
➔ Cloud-Grundlagen			
➔ Cloud-Strategie			

3.3.2. Vereinbarungen zur Servicequalität

3.3.2.1. Servicemanagement

3.3.2.1.1. IT-Service-Management

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider betreibt ein IT-Service-Management (ITSM), das sich an anerkannten ITSM-Standards orientiert und die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.</p> <p>Die Aktualität, Vollständigkeit und Wirksamkeit des ITSM und der dokumentierten Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services werden im Rahmen eines jährlichen Auditprogramms auditiert.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9 <input checked="" type="checkbox"/> ITIL			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ IT-Servicemanagement			

3.3.2.1.2. IT-Service-Managementzertifizierung

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verfügt über eine gültige ITSM-Zertifizierung einer akkreditierten Zertifizierungsstelle. In der Anwendbarkeitserklärung (Statement of Applicability) ist ausgewiesen, dass das ITSM die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden bei der Erneuerung bzw. Verlängerung eine Kopie des gültigen Zertifikats und der Anwendbarkeitserklärung zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Zertifikats durch die Zertifizierungsstelle.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Zertifizierungsstandards➔ Prüfungsstandards			

3.3.2.1.3. Kontinuitäts- und Verfügbarkeitsmanagement

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die Verfügbarkeit des Cloud-Services wird auf Basis von festgelegten Kontinuitäts- und Verfügbarkeitsmanagementprozessen, die sich an anerkannten ITSM-Standards orientieren, und auf Basis festgelegter Pläne sichergestellt, getestet und laufend überwacht.</p> <p>Der Cloud-Service-Kunde wird im Fall einer schwerwiegenden Störung oder eines Ausfalls des Cloud-Services umgehend informiert. Es ist klar zu regeln, für welche Arten von Störungen und Ausfällen eine Informierung vorzunehmen ist. Zudem sind die dafür zu nutzenden Informationskanäle vorab festzulegen.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9 <input checked="" type="checkbox"/> ITIL			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ IT-Servicemanagement			

3.3.2.1.4. Kapazitätsmanagement

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die Planung, Bereitstellung und laufende Überwachung der erforderlichen Kapazitäten und Performance des Cloud-Services erfolgt auf Basis von festgelegten Kapazitätsmanagementprozessen, die sich an anerkannten ITSM-Standards orientieren.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9 <input checked="" type="checkbox"/> ITIL			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ IT-Servicemanagement			

3.3.2.1.5. Störungs- und Problemmanagement

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Auftretende Störungen und Probleme des Cloud-Services werden auf Basis von festgelegten Störungs- und Problemmanagementprozessen bearbeitet, die sich an anerkannten ITSM-Standards ori-</p>			

entieren.

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die Regelungen hinsichtlich Meldung, Klassifizierung, Bearbeitung, Priorisierung, Behebung und Eskalation zur Verfügung.

Referenzierte Standards

- ISO/IEC 20000-1 und ISO/IEC 20000-9
- ITIL

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ IT-Servicemanagement

3.3.2.1.6. Konfigurationsmanagement

Schutzbedarf

- | | | | |
|-------------------------------------|--|--|---|
| <input type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|-------------------------------------|--|--|---|

Anforderung

Die Konfiguration und Dokumentation der für die Bereitstellung des Cloud-Services relevanten IT-Systeme und Komponenten erfolgt auf Basis von festgelegten Konfigurationsmanagementprozessen, die sich an anerkannten ITSM-Standards orientieren.

Referenzierte Standards

- ISO/IEC 20000-1 und ISO/IEC 20000-9
- ITIL

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ IT-Servicemanagement

3.3.2.1.7. Änderungs- und Versionsmanagement

Schutzbedarf

- | | | | |
|--|--|--|---|
| <input checked="" type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|--|--|--|---|

Anforderung

Die Planung, Dokumentation, Koordination, Qualitätssicherung, Genehmigung und Überwachung von Änderungen und neuen Versionen des Cloud-Services erfolgen auf Basis von festgelegten Änderungs- und Versionsmanagementprozessen, die sich an anerkannten ITSM-Standards orientieren.

Der Cloud-Service-Kunde wird über Änderungen und neue Versionen vorab informiert. Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die Regelungen hinsichtlich Information (sowie etwaiger Freigaben), Vorlaufzeiten, Wechselpflicht und Beschreibung der Änderungen zur Verfügung.

Referenzierte Standards

- ISO/IEC 20000-1 und ISO/IEC 20000-9

<input checked="" type="checkbox"/> ITIL
Weiterführende Informationen
<ul style="list-style-type: none"> ➔ Anforderungen an Cloud-Services ➔ IT-Servicemanagement

3.3.2.1.8. Skalierbarkeit

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Das Cloud-Service verfügt über eine ausreichende Skalierbarkeit, die dem Cloud-Service-Kunden die Nutzung der zugesicherten Leistungs-, Performance- und Kapazitätsmengen gewährleistet. Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen zu den möglichen Bandbreiten hinsichtlich Rechenleistung, Arbeitsspeicher, Speicherplatz, Netzwerkbandbreite und Benutzeranzahl zur Verfügung.</p>			
Referenzierte Standards			
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9 <input checked="" type="checkbox"/> ITIL 			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Anforderungen an Cloud-Services ➔ IT-Servicemanagement 			

3.3.2.1.9. Portabilität

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Das Cloud-Service verfügt über eine ausreichende Portabilität der verarbeiteten, gespeicherten und gesicherten Daten, die jederzeit einen uneingeschränkten Datenexport unter Beibehaltung aller logischen Relationen gewährleistet.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die zugesicherten Datenexportformate zur Verfügung.</p>			
Referenzierte Standards			
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> IEEE P2301 <input checked="" type="checkbox"/> ISO/IEC 19941 			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Interoperabilität und Portabilität 			

3.3.2.1.10. Interoperabilität

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Das Cloud-Service unterstützt Interoperabilitätsstandards, um eine ausreichende Kompatibilität mit anderen Cloud-Services sicherzustellen.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die zugesicherten Systemschnittstellen und Protokolle zur Verfügung.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> IEEE P2301, IEEE P2302 <input checked="" type="checkbox"/> ISO/IEC 17203, ISO/IEC 17826, ISO/IEC 19831, ISO/IEC 19941, ISO/IEC 19944 <input checked="" type="checkbox"/> KMIP <input checked="" type="checkbox"/> OCCI			
Weiterführende Informationen			
↪ Interoperabilität und Portabilität			

3.3.2.2. Service Level

3.3.2.2.1. Service Level Agreement

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die zugesicherten Leistungsparameter des Cloud-Services werden in einem schriftlichen Service Level Agreement zwischen Cloud-Service-Provider und Cloud-Service-Kunden vertraglich vereinbart.</p> <p>Dazu zählen insb. folgende Vereinbarungen:</p> <ul style="list-style-type: none"> ▪ Allgemeine Service Level-Parameter <ul style="list-style-type: none"> ▪ Funktionen, Benutzer-Support, Performance, Kapazitäten und Verfügbarkeit ▪ Reaktions- bzw. Antwortzeiten, Behebungs- bzw. Wiederherstellungszeiten ▪ Maximale Ausfallshäufigkeit ▪ Messtransaktionen, -punkte und -frequenzen ▪ Regelungen i. Z. m. Wartungsfenstern und Notfalländerungen ▪ Standards und Zertifizierungen <ul style="list-style-type: none"> ▪ Verwendete IT-Service-Managementstandards ▪ Vorhandene IT-Service-Managementzertifizierungen ▪ Unterstützte Portabilitätsstandards ▪ Unterstützte Interoperabilitätsstandards ▪ Vertragsverletzungen <ul style="list-style-type: none"> ▪ Pönale bei Verletzung der vertraglichen Parameter <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die getroffenen Maßnahmen zur Sicherstellung der Servicequalität zur Verfügung.</p>			

Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9 <input checked="" type="checkbox"/> ITIL			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Anforderungen an Cloud-Services ➔ IT-Servicemanagement ➔ Service Level Agreements 			

3.3.2.2.2. Operational Level Agreement

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die vertraglich vereinbarten Leistungsparameter des Cloud-Services sind durch den Cloud-Service-Provider mittels schriftlicher Operational Level Agreements mit organisationsinternen Einheiten und etwaigen weiteren Dienstleistern und Subdienstleistern abgesichert.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9 <input checked="" type="checkbox"/> ITIL			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Anforderungen an Cloud-Services ➔ IT-Servicemanagement ➔ Service Level Agreements 			

3.3.2.2.3. Service Level Reporting

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die vertraglich vereinbarten Leistungsparameter des Cloud-Services werden vereinbarungsgemäß vermessen und dokumentiert. Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden monatlich einen schriftlichen Bericht der Vermessungsergebnisse zur Verfügung.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 20000-1 und ISO/IEC 20000-9 <input checked="" type="checkbox"/> ITIL			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Anforderungen an Cloud-Services ➔ IT-Servicemanagement ➔ Service Level Agreements 			

3.3.3. Vereinbarungen zur Informationssicherheit

3.3.3.1. Sicherheitsmanagement

3.3.3.1.1. Informationssicherheits-Managementsystem

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider betreibt ein Informationssicherheits-Managementsystem (ISMS), das sich an anerkannten Sicherheitsstandards orientiert und die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.</p> <p>Verbindliche Sicherheitsrichtlinien zur Steuerung und Überwachung des ISMS sowie zur Festlegung von Sicherheitsanforderungen für Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services sind dokumentiert und kommuniziert. Die Festlegung der organisatorischen und technischen Sicherheitsmaßnahmen des Cloud-Services erfolgt auf Basis von festgelegten Risiko-Managementprozessen, die sich an anerkannten Sicherheitsstandards orientieren. Für Personen, die an der Erbringung des Cloud-Services beteiligt sind, finden regelmäßige und verbindliche Sicherheits-schulungen statt. Dies gilt auch für Personal etwaiger weiterer Dienstleister und Subdienstleister.</p> <p>Die Aktualität, Vollständigkeit und Wirksamkeit des ISMS, der Sicherheitsrichtlinien und der organisatorischen und technischen Sicherheitsmaßnahmen des Cloud-Services werden im Rahmen eines jährlichen Auditprogramms auditiert.</p>			
Referenzierte Standards			
<p>Informationssicherheits-Managementstandards:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017<input checked="" type="checkbox"/> Österreichisches Informationssicherheitshandbuch<input checked="" type="checkbox"/> BSI-Standard 100-1, BSI-Standard 100-2 und BSI IT-Grundschutz <p>Risiko-Managementstandards:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> ISO/IEC 27005<input checked="" type="checkbox"/> ISO 31000<input checked="" type="checkbox"/> ONR 49000<input checked="" type="checkbox"/> BSI 100-3 <p>Auditstandards:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> ISO 19011, ISO/IEC 27007 und <input checked="" type="checkbox"/> ISO/IEC TR 27008<input checked="" type="checkbox"/> SP 800-115			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ Informationssicherheitsmanagement➔ Risikomanagement➔ Auditierung und Test			

3.3.3.1.2. Informationssicherheits-Gütesiegel

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verfügt über ein anerkanntes gültiges Informationssicherheits-Gütesiegel, das die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden bei der Erneuerung bzw. Verlängerung eine Kopie des gültigen Gütesiegels zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Zertifikats.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> CSA STAR <input checked="" type="checkbox"/> ESCloud Label <input checked="" type="checkbox"/> EuroCloud StarAudit <input checked="" type="checkbox"/> Trusted Cloud-Service			
Weiterführende Informationen			
→ Gütesiegel			

3.3.3.1.3. Informationssicherheits-Managementsystemzertifizierung

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verfügt über eine gültige ISMS-Zertifizierung einer akkreditierten Zertifizierungsstelle. In der Anwendbarkeitserklärung (Statement of Applicability) ist ausgewiesen, dass das ISMS die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden bei der Erneuerung bzw. Verlängerung eine Kopie des gültigen Zertifikats und der Anwendbarkeitserklärung zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Zertifikats durch die Zertifizierungsstelle.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden den Bericht des jährlich durchgeführten Überwachungs- bzw. Zertifizierungsaudits zur Verfügung, der i. Z. m. dem Cloud-Service Auskunft über das Auditergebnis und etwaige Verbesserungshinweise und Abweichungen gibt.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001 <input checked="" type="checkbox"/> ISO/IEC 27001 auf Basis des BSI IT-Grundschutzes			
Weiterführende Informationen			
→ Zertifizierungsstandards → Prüfungsstandards			

3.3.3.1.4. Produkt- und Systemzertifizierungen

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verfügt über eine gültige Produktzertifizierung des Cloud-Services einer akkreditierten Zertifizierungsstelle.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden bei der Erneuerung bzw. Verlängerung eine Kopie des gültigen Zertifikats zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Zertifikats durch die Zertifizierungsstelle.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27018 <input checked="" type="checkbox"/> ISO/IEC 15408 <input checked="" type="checkbox"/> ÖNORM A7700			
Weiterführende Informationen			
↪ Zertifizierungsstandards			

3.3.3.1.5. Benennung eines zentralen Ansprechpartners

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider benennt eine zentrale Ansprechpartnerin bzw. einen zentralen Ansprechpartner (Informationssicherheitsbeauftragte/n), der dem Cloud-Service-Kunden für alle Belange der Informationssicherheit beim Cloud-Service-Provider und etwaiger weiterer Dienstleister und Subdienstleister zur Verfügung steht und stellt dem Cloud-Service-Kunden dessen Kontaktdaten zur Verfügung, einschl. Name, Telefonnummer und E-Mail-Adresse.</p>			
Weiterführende Informationen			
↪ Anforderungen an Cloud-Services ↪ Informationssicherheitsmanagement			

3.3.3.1.6. Verwaltung von Benutzerkennungen, Rollen und Rechten

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Zur Sicherstellung einer kontrollierten und nachvollziehbaren Verwaltung von Benutzerkennungen, Rollen und Rechten ist ein Registrierungs- und Provisionierungsverfahren umgesetzt, das den gesamten Lebenszyklus umfasst.</p> <p>Dazu zählen</p>			

<ul style="list-style-type: none"> ▪ die Registrierung und De-Registrierung von Benutzerinnen und Benutzern, ▪ die Vergabe, zeitliche Beschränkung, Änderung, Prüfung, Deaktivierung, Entziehung und Löschung von Kennungen, Rollen und Rechten, ▪ die Vergabe, Bereitstellung, Zurücksetzung und der Widerruf von Zugangsdaten sowie ▪ die Protokollierung der durchgeführten Aktivitäten.
Referenzierte Standards
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017
Weiterführende Informationen
<ul style="list-style-type: none"> ➔ Identity- und Access-Management ➔ E-Government-Konventionen

3.3.3.1.7. Authentifizierung und Autorisierung

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Um ausschließlich autorisierte Zugriffe auf das Cloud-Service sicherzustellen, sind geeignete Zugriffskontrollen in Form von Authentifizierungs- und Autorisierungsverfahren umgesetzt. Eine Session-Timeout-Funktion stellt zudem sicher, dass bestehende Sessions nach einem festgelegten Zeitlimit geschlossen und Zugriffe bis zu einer neuerlichen Anmeldung verhindert werden.</p> <p>Bei der Verwendung von Passwörtern werden geeignete Verfahren eingesetzt, die eine entsprechende Passwortkomplexität (Mindestlänge, Sonderzeichen etc.) und eine Durchsetzung von regelmäßigen Passwortänderungen gewährleisten. Das Erraten von Passwörtern, z. B. mittels Brute-Force-Methoden, wird durch geeignete Sperrmechanismen unterbunden.</p> <p>Dies gilt für Benutzer- und Administratorzugänge.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Identity- und Access-Management ➔ E-Government-Konventionen 			

3.3.3.1.8. Zwei-Faktor-Authentifizierung

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die Zugriffskontrolle des Cloud-Services verwendet eine Zwei-Faktor-Authentifizierungsmethode. Dies gilt für Benutzer- und Administratorzugänge.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			

Weiterführende Informationen

- ⇒ Identity- und Access-Management
- ⇒ E-Government-Konventionen

3.3.3.1.9. Datenverschlüsselung

Schutzbedarf

- | | | | |
|-------------------------------------|---------------------------------|--|---|
| <input type="checkbox"/> Unkritisch | <input type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|-------------------------------------|---------------------------------|--|---|

Anforderung

Zur Sicherstellung der Vertraulichkeit der verarbeiteten Daten des Cloud-Services ist eine durchgängige Datenverschlüsselung unter Verwendung geeigneter Verschlüsselungsalgorithmen und Schlüssel-längen umgesetzt, die den gesamten Lebenszyklus der Daten, einschl. der Speicherung und Sicherung, umfasst und einen unbefugten Zugriff auf Daten im Klartext verhindert.

Referenzierte Standards

- ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017
- BSI TR-02102-1

Weiterführende Informationen

- ⇒ Kryptografie
- ⇒ E-Government-Konventionen

3.3.3.1.10. Rechenzentrumsicherheit

Schutzbedarf

- | | | | |
|-------------------------------------|--|--|---|
| <input type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|-------------------------------------|--|--|---|

Anforderung

Die Implementierung der zur Bereitstellung des Cloud-Services erforderlichen IT-Systeme und Komponenten erfolgt ausschließlich in ausreichend abgesicherten Systemräumen. Die Absicherung umfasst insb. folgende Maßnahmen:

- eine entsprechende Sicherung von Wänden, Fenstern und Türen
- einen ausreichenden Zutrittsschutz (z. B. sichere Authentifizierungsverfahren, Vereinzelungsanlage, Bewegungsmelder und Videoüberwachung)
- eine unterbrechungsfreie Stromversorgung (z. B. USV und Notstromaggregate)
- eine ausreichende Netzwerkanbindung und sichere Netzwerkverkabelung
- eine ausreichende Klimatisierung (Raumtemperatur und -feuchte)
- einen ausreichenden Brandschutz (Brandalarmierung und -bekämpfung)

Zur Einhaltung der festgelegten Verfügbarkeitsparameter des Cloud-Services sind geeignete Vorsorgemaßnahmen, Wiederherstellungsstrategien und Notfallpläne umgesetzt und getestet. Dazu zählen insb. unterstützende Versorgungseinrichtungen, Brandschutz, Redundanz der IT-Infrastruktur und der Netz- und Telekommunikationseinrichtungen sowie Parallel- bzw. Ausweichstandorte. Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die getroffenen Maßnahmen zur Verfügung.

Referenzierte Standards

- ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017
- EN 50600
- ANSI/TIA 942

Weiterführende Informationen

- ➔ Rechenzentren

3.3.3.1.11. Rechenzentrumsicherheits-Zertifizierung

Schutzbedarf

- | | | | |
|-------------------------------------|---------------------------------|-------------------------------|---|
| <input type="checkbox"/> Unkritisch | <input type="checkbox"/> Normal | <input type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|-------------------------------------|---------------------------------|-------------------------------|---|

Anforderung

Der Cloud-Service-Provider verfügt über eine gültige Rechenzentrumsicherheits-Zertifizierung einer akkreditierten Zertifizierungsstelle.

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden bei der Erneuerung bzw. Verlängerung eine Kopie des gültigen Zertifikats und der Anwendbarkeitserklärung (Statement of Applicability) zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Zertifikats durch die Zertifizierungsstelle.

Referenzierte Standards

- EN 50600
- ANSI/TIA 942

Weiterführende Informationen

- ➔ Zertifizierungsstandards
- ➔ Prüfungsstandards

3.3.3.1.12. Update- und Patch-Management

Schutzbedarf

- | | | | |
|--|--|--|---|
| <input checked="" type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|--|--|--|---|

Anforderung

Die Koordination und zeitgerechte Behebung von Sicherheitsschwachstellen in Hardware- und Softwarekomponenten des Cloud-Services erfolgt auf Basis von festgelegten Update- und Patch-Managementprozessen, die sich an anerkannten Sicherheitsstandards orientieren und eine entsprechende Qualitätssicherung in Form von Funktions- und Kompatibilitätstests sicherstellen.

Referenzierte Standards

- ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ Informationssicherheitsmanagement

3.3.3.1.13. Mandanten- und Systemtrennung

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Das Cloud-Service verfügt über eine vollständige und durchgängige Mandantentrennung, die dem Cloud-Service-Kunden hinsichtlich der genutzten Infrastruktur und der verarbeiteten, gespeicherten und gesicherten Daten einen dedizierten Mandantenbereich und eine entsprechende Abgrenzung von anderen Mandanten gewährleistet. Dies gilt insb. für</p> <ul style="list-style-type: none"> ▪ die Administration und Provisionierung von Benutzerkennungen, Rollen und Rechten, ▪ die verarbeiteten Anwendungs- und Protokolldaten sowie ▪ die verwendeten IT-Anwendungen, Betriebssysteme, Datenbanken, Speicher- und Backupsysteme und Netzwerksegmente. <p>Die Produktivumgebung des Cloud-Services ist strikt von anderen Systemumgebungen, wie z. B. Schulungs-, Qualitätssicherungs-, Integrations-, Test- und Entwicklungsumgebungen, getrennt.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Anforderungen an Cloud-Services ➔ Informationssicherheitsmanagement 			

3.3.3.1.14. Schadsoftware-Erkennung und Abwehr

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Zur Erkennung und Abwehr von Schadsoftware und nicht genehmigtem mobilen Programmcode sind geeignete Virenschutzverfahren und entsprechende Alarmierungs- und Reaktionsprozesse umgesetzt. Die eingesetzten Produkte (Engines und Agents) werden auf dem aktuellsten Versionsstand gehalten. Die eingesetzten Virendefinitionen werden (zumindest) tagesaktuell gehalten, wobei diese zur Vermeidung von etwaigen Beeinträchtigungen aufgrund von Fehlfunktionen vor dem Rollout mittels False-Positive-Checks geprüft werden.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Anforderungen an Cloud-Services ➔ Informationssicherheitsmanagement 			

3.3.3.1.15. Sandbox-Virenschanner

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Zur Erhöhung der Erkennungsrate des mehrstufigen Virenschutzes des Cloud-Services sind zusätzliche Virenschanner auf Basis der Sandbox-Technologie einzusetzen.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ Informationssicherheitsmanagement			

3.3.3.1.16. Datensicherung

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Zur Vermeidung von Datenverlusten des Cloud-Services werden geeignete Datensicherungsverfahren eingesetzt. Die Wiederherstellbarkeit der gesicherten Daten wird regelmäßig überprüft.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ Informationssicherheitsmanagement			

3.3.3.1.17. Protokollierung

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Systemrelevante Ereignisse und Fehler des Cloud-Services, alle erfolgten Anmeldungen und fehlgeschlagenen Anmeldeversuche sowie sämtliche Benutzer- und Administrationsaktivitäten werden protokolliert.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ Informationssicherheitsmanagement➔ E-Government-Konventionen			

➔ Weitere technische Spezifikationen

3.3.3.1.18. Sicherheitsschwachstellen-Monitoring

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Um bekannt gewordene Sicherheitsschwachstellen in Hardware- und Softwarekomponenten des Cloud-Services so rasch wie möglich identifizieren, bewerten und beheben zu können, führt der Cloud-Service-Provider ein Monitoring einschlägiger Quellen sowie regelmäßige Schwachstellen-Scans durch. Die Dokumentation von Sicherheitsschwachstellen, Behebungsmaßnahmen und Workarounds erfolgt in einem dafür vorgesehenen Ticketsystem. Die Bewertung von Sicherheitsschwachstellen erfolgt auf Basis anerkannter Sicherheitsstandards.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017 <input checked="" type="checkbox"/> X.1521, X.1524, X.1525, X.1526, X.1528, X.1544			
Weiterführende Informationen			
➔ Sicherheitsschwachstellenmanagement			

3.3.3.1.19. Penetrationstests

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Zur Identifizierung und Behebung von Sicherheitsschwachstellen im Programm-Quellcode oder in der Systemkonfiguration des Cloud-Services werden vor der Inbetriebnahme und bei allfälligen Änderungen Penetrationstests durchgeführt.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
➔ Applikationssicherheit ➔ Systemhärtung ➔ Systemevaluierung			

3.3.3.1.20. Netzwerksicherheit

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Zur Sicherstellung einer ausreichenden Netzwerksicherheit des Cloud-Services ist eine entsprechende Netzwerktrennung mittels Netzwerksegmenten bzw. Netzwerkzonen und erforderlichenfalls Demilita-			

risierten Zonen umgesetzt. Die Kontrolle des Netzwerkverkehrs erfolgt mittels Netzwerk-Firewalls, die Erkennung von netzwerkbasierter Angriffen mittels Netzwerk-Intrusion-Detection-Systemen bzw. Netzwerk-Intrusion-Prevention-Systemen.

Die Netzwerkkommunikation des Cloud-Services wird durch geeignete End-to-End-Verschlüsselungsalgorithmen und Schlüssellängen abgesichert. Dies gilt für Benutzer- und Administrationszugänge sowie für etwaige Fernwartungszugänge. Die dabei verwendeten Zertifikate werden beim Verbindungsaufbau einer entsprechenden Validierung unterzogen, die sowohl eine kryptografische Verifikation als auch eine Gültigkeitsabfrage über entsprechende Verzeichnisdienste inkludiert. Bei der Auswahl und regelmäßigen Aktualisierung geeigneter Protokollversionen und Cipher-Suites werden die aktuellen Sicherheitsempfehlungen anerkannter Organisationen eingehalten. Für die Kommunikation zwischen Cloud-Service-Kunden und Cloud-Service-Provider werden ausschließlich Zertifikate von öffentlichen Vertrauensdiensteanbietern eingesetzt.

Referenzierte Standards

- ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017
- BSI TR-02102-1, BSI TR-02102-2, BSI TR-02102-3, BSI TR-02102-4
- A-SIT Empfehlungen für Behörden
- PVP-SMA

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ Informationssicherheitsmanagement
- ➔ Kryptografie
- ➔ E-Government-Konventionen

3.3.3.1.21. Denial of Service-Abwehrsysteme

Schutzbedarf

- | | | | |
|-------------------------------------|---------------------------------|--|---|
| <input type="checkbox"/> Unkritisch | <input type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|-------------------------------------|---------------------------------|--|---|

Anforderung

Zur Erkennung und Abwehr von Denial of Service (DoS)-Angriffen werden entsprechende DoS-Abwehrsysteme eingesetzt.

Referenzierte Standards

- ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ Informationssicherheitsmanagement

3.3.3.1.22. Web Application Firewalls

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Zur Erkennung und Abwehr von Angriffen auf Applikationsebene werden geeignete Web Application Firewalls (WAF) eingesetzt.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Anforderungen an Cloud-Services➔ Informationssicherheitsmanagement➔ Applikationssicherheit			

3.3.3.1.23. Systemhärtung

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die eingesetzten Systemkomponenten des Cloud-Services werden vor der Inbetriebnahme und bei allfälligen Änderungen einer geeigneten Systemhärtung unterzogen, bei der insb. Softwarebestandteile, Funktionen und Dienste, die nicht zwingend notwendig sind, entfernt bzw. deaktiviert werden. Bei der Festlegung der Systemhärtungsmaßnahmen werden die aktuellen Sicherheitsempfehlungen anerkannter Organisationen eingehalten.</p> <p>Firmware und Software werden am aktuellen Versionsstand gehalten. Darüber hinaus wird der administrative Zugang zu System- und Netzwerkkomponenten durch geeignete Maßnahmen abgesichert, insb. durch sichere Authentifizierungsverfahren, Session Timeouts und Management VLANs.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017 <input checked="" type="checkbox"/> NIST SP 800-70 Rev. 3 <input checked="" type="checkbox"/> OWASP <input checked="" type="checkbox"/> CIS-Benchmarks			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Applikationssicherheit➔ Systemhärtung➔ Systemevaluierung			

3.3.3.1.24. Systems Development Life Cycle

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Um sicherzustellen, dass wesentliche Sicherheitsaspekte bereits im Entwicklungsprozess berücksichtigt werden, erfolgt die Entwicklung des Cloud-Services auf Basis eines dokumentierten Systems Development Life Cycle (SDLC)-Prozesses, der sich an anerkannten Sicherheitsstandards orientiert und entsprechende Analyse-, Design-, Review- und Testvorgaben vorsieht.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017			
Weiterführende Informationen			
➔ Applikationssicherheit			

3.3.3.1.25. Secure Coding-Standards

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Zur Vermeidung von Sicherheitsschwachstellen im Programm-Quellcode des Cloud-Services werden im Entwicklungsprozess anerkannte Secure Coding-Standards angewendet und eingehalten. Beim Einsatz von Drittkomponenten, wie z. B. Programm-Bibliotheken, wird sichergestellt, dass diese aus vertrauenswürdigen Quellen bezogen, auf Schadsoftware geprüft und entsprechend lizenziert wurden.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017 <input checked="" type="checkbox"/> OWASP			
Weiterführende Informationen			
➔ Applikationssicherheit			

3.3.3.1.26. Source Code-Analysen

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
Zur Identifizierung und Behebung von Sicherheitsschwachstellen im Programm-Quellcode des Cloud-Services werden im Rahmen des Entwicklungsprozesses automatisierte Source Code-Analysen durchgeführt.			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017 <input checked="" type="checkbox"/> OWASP			

Weiterführende Informationen

→ Applikationssicherheit

3.3.3.1.27. Sicherheitsvorfall-Management und Informationspflicht

Schutzbedarf

Unkritisch Normal Hoch Sehr hoch

Anforderung

Die Überwachung, Bewertung, Dokumentation, Kommunikation und Eskalation von Sicherheitsvorfällen erfolgt auf Basis von festgelegten Sicherheitsvorfall-Managementprozessen, die sich an anerkannten Sicherheitsstandards orientieren.

Der Cloud-Service-Provider informiert den Cloud-Service-Kunden unverzüglich über aufgetretene Sicherheitsvorfälle i. Z. m. dem Cloud-Service und stellt ihm alle erforderlichen Informationen zur Verfügung, die zur Klärung des Sachverhalts und Aufrechterhaltung des Betriebs sowie zur Erfüllung seiner Informationspflichten notwendig sind.

Referenzierte Standards

ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017
 ISO/IEC 27035

Weiterführende Informationen

→ Sicherheitsvorfallmanagement

3.3.3.1.28. Notfall-Management und Informationspflicht

Schutzbedarf

Unkritisch Normal Hoch Sehr hoch

Anforderung

Die Sicherstellung einer angemessenen Ausfallssicherheit und die Festlegung von adäquaten Prozessen zur Bewältigung von Notfällen und Krisen erfolgt auf Basis von festgelegten Notfall-Managementprozessen, die sich an anerkannten Sicherheitsstandards orientieren.

Der Cloud-Service-Provider informiert den Cloud-Service-Kunden unverzüglich über aufgetretene Notfälle i. Z. m. dem Cloud-Service und stellt ihm alle erforderlichen Informationen zur Verfügung, die zur Klärung des Sachverhalts und Aufrechterhaltung des Betriebs sowie zur Erfüllung seiner Informationspflichten notwendig sind.

Referenzierte Standards

ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017
 ISO/IEC 27031
 BSI 100-4

Weiterführende Informationen

→ Business Continuity Management

3.3.3.1.29. Notfall-Managementzertifizierung

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verfügt über eine gültige Business Continuity-Management (BCM)-Zertifizierung einer akkreditierten Zertifizierungsstelle. In der Anwendbarkeitserklärung (Statement of Applicability) ist ausgewiesen, dass das BCM die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden bei der Erneuerung bzw. Verlängerung eine Kopie des gültigen Zertifikats und der Anwendbarkeitserklärung zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Zertifikats durch die Zertifizierungsstelle.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> ISO 22301			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Zertifizierungsstandards ➔ Prüfungsstandards 			

3.3.3.2. Security Level

3.3.3.2.1. Security Level Agreement

Schutzbedarf			
<input checked="" type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die zugesicherten Sicherheitsparameter des Cloud-Services werden in einem schriftlichen Security Level Agreement zwischen Cloud-Service-Provider und Cloud-Service-Kunden vertraglich vereinbart.</p> <p>Dazu zählen insb. folgende Vereinbarungen:</p> <ul style="list-style-type: none"> ▪ Allgemeine Security Level-Parameter <ul style="list-style-type: none"> ▪ Wiederanlaufzeit (RTO) und Wiederanlaufniveau, max. tolerierbare Ausfallszeit (MTPD) und max. zulässiger Datenverlust (RPO) ▪ Schadsoftware-Erkennung und Abwehr <ul style="list-style-type: none"> ▪ Geschützte Schnittstellen (z. B. APIs), Funktionen (z. B. Upload) und strukturelle Einheiten (z. B. Dateien und Laufwerke) ▪ Eingesetzte Technologien (z. B. signaturbasierte Virens Scanner, Integritätsüberwachung, Reencoding, künstliche Intelligenz, Sandboxing) ▪ Datensicherung <ul style="list-style-type: none"> ▪ Umfang, Art (inkrementelle Sicherung bzw. Vollsicherung) und Häufigkeit (Intervall und Zeitpunkt), Aufbewahrungsdauer und -ort sowie Dauer der Datenwiederherstellung ▪ Schutz der Datensicherungen vor unberechtigtem Zugriff und Verfälschung ▪ Protokollierung <ul style="list-style-type: none"> ▪ Umfang und Struktur, Aufbewahrungsdauer und -ort sowie Löschrufen 			

- Schutz der Protokolldaten vor unberechtigtem Zugriff und Verfälschung
- Überwachungs- und Auswertungsmodalitäten
- Schwachstellen-Management
 - Reaktions- und Behebungszeiten bei Sicherheitsschwachstellen (nach Kritikalitätsstufen)
- Penetrationstests und Secure Code-Analysen (sofern zutreffend)
 - Intervalle der durchgeführten Tests und Analysen
- Kryptografie
 - Verwendete Verschlüsselungsalgorithmen und Schlüssellängen bei der Datenübermittlung
 - Verwendete Verschlüsselungsalgorithmen und Schlüssellängen bei der Datenspeicherung
- Systemhärtung
 - Verwendete Configuration Baselines
- Standards, Zertifizierungen und Gütesiegel (sofern zutreffend)
 - Verwendete Informationssicherheits-Managementsystemstandards
 - Vorhandene Informationssicherheits-Gütesiegel
 - Vorhandene Informationssicherheits-Managementsystemzertifizierungen
 - Verfügbare Produkt- und Systemzertifizierungen
 - Vorhandene Rechenzentrumsicherheits-Zertifizierungen
 - Verwendete System Development- und Secure Coding-Standards
 - Vorhandene Notfall-Managementzertifizierungen
- Vertragsverletzungen
 - Pönale bei Verletzung der vertraglichen Parameter

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die getroffenen Maßnahmen zur Sicherstellung der Informationssicherheit zur Verfügung.

Referenzierte Standards

ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ Informationssicherheitsmanagement

3.3.3.2.2. Sicherheitsanforderungen und Sicherheitskonzept

Schutzbedarf

<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
-------------------------------------	--	--	---

Anforderung

Der Cloud-Service-Kunde stellt dem Cloud-Service-Provider eine schriftliche Dokumentation der festgelegten Sicherheitsanforderungen und Abnahmekriterien zur Verfügung, die durch den Cloud-Service-Provider bei der Festlegung, Umsetzung und Überprüfung der organisatorischen und technischen Sicherheitsmaßnahmen des Cloud-Services zu erfüllen sind.

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden vor der Inbetriebnahme des Cloud-Services sowie bei allfälligen Änderungen eine schriftliche Dokumentation über die umgesetzten und überprüften Sicherheitsmaßnahmen in Form eines Sicherheitskonzepts und Abnahmetestprotokolls zur Verfügung.

Referenzierte Standards

ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ Informationssicherheitsmanagement

3.3.3.2.3. Sicherheitskennzahlen

Schutzbedarf

Unkritisch Normal Hoch Sehr hoch

Anforderung

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden monatlich einen schriftlichen Sicherheitskennzahlenbericht zur Verfügung, der Auskunft über die Wirksamkeit wesentlicher organisatorischer und technischer Sicherheitsmaßnahmen gibt.

Die Abstimmung und Festlegung der zu berichtenden Kennzahlen erfolgt einvernehmlich zwischen Cloud-Service-Kunden und Cloud-Service-Provider.

Referenzierte Standards

ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27017

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ Informationssicherheitsmanagement

3.3.4. Vereinbarungen zum Datenschutz

3.3.4.1. Datenschutzmanagement

3.3.4.1.1. Datenschutz-Managementsystem

Schutzbedarf

Unkritisch Normal Hoch Sehr hoch

Anforderung

Der Cloud-Service-Provider betreibt ein Datenschutz-Managementsystem (DSMS), das sich an anerkannten Datenschutzstandards orientiert und die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.

Verbindliche Datenschutzrichtlinien zur Steuerung und Überwachung des DSMS sowie zur Festlegung von Datenschutzerfordernungen für Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services sind dokumentiert und kommuniziert. Die Festlegung der organisatorischen und technischen Datenschutzmaßnahmen des Cloud-Services erfolgt auf Basis von festgelegten Risiko-Managementprozessen, die sich an anerkannten Datenschutzstandards orientieren. Für Personen, die an der Erbringung des Cloud-Services beteiligt sind, finden regelmäßige und verbindliche Datenschutzeschulungen statt. Dies gilt auch für Personal etwaiger weiterer Dienstleister und Subdienstleister.

Die Aktualität, Vollständigkeit und Wirksamkeit des DSMS, der Datenschutzrichtlinien und der organisatorischen und technischen Datenschutzmaßnahmen des Cloud-Services werden im Rahmen eines jährlichen Auditprogramms auditiert.

Referenzierte Standards

Datenschutz-Managementstandards

- BS 10012
- ISO/IEC 27001 iVm ISO/IEC 27018, ISO/IEC 29151

Risiko-Managementstandards:

- ISO/IEC 27005
- ISO 31000
- ONR 49000
- BSI 100-3

Datenschutz-Folgenabschätzung:

- ISO/IEC 29134

Auditstandards:

- ISO 19011, ISO/IEC 27007 und ISO/IEC TR 27008
- SP 800-115

Weiterführende Informationen

- ➔ Anforderungen an Cloud-Services
- ➔ Datenschutzmanagement
- ➔ Datenschutzfolgenabschätzung
- ➔ Rahmenwerke, Handbücher und Kataloge

3.3.4.1.2. Datenschutz-Gütesiegel

Schutzbedarf

- | | | | |
|-------------------------------------|--|--|---|
| <input type="checkbox"/> Unkritisch | <input checked="" type="checkbox"/> Normal | <input checked="" type="checkbox"/> Hoch | <input checked="" type="checkbox"/> Sehr hoch |
|-------------------------------------|--|--|---|

Anforderung

Der Cloud-Service-Provider verfügt über ein anerkanntes gültiges Datenschutz-Gütesiegel, das die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.

Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden regelmäßig eine Kopie des Gütesiegels zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Gütesiegels.

Referenzierte Standards

- EuroPriSe

Weiterführende Informationen

- ➔ Gütesiegel

3.3.4.1.3. Datenschutz-Zertifizierung

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider verfügt über eine gültige Datenschutz-Zertifizierung einer akkreditierten Zertifizierungsstelle. In der Anwendbarkeitserklärung (Statement of Applicability) ist ausgewiesen, dass die Datenschutz-Zertifizierung die Entwicklungs-, Inbetriebnahme- und Betriebsprozesse des Cloud-Services vollständig umfasst.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden bei der Erneuerung bzw. Verlängerung eine Kopie des gültigen Zertifikats und der Anwendbarkeitserklärung zur Verfügung und informiert den Cloud-Service-Kunden umgehend über eine etwaige Zurückziehung oder Aussetzung des Zertifikats durch die Zertifizierungsstelle.</p> <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden den Bericht des jährlich durchgeführten Überwachungs- bzw. Zertifizierungsaudits zur Verfügung, der i. Z. m. dem Cloud-Service Auskunft über das Auditergebnis und etwaige Verbesserungshinweise und Abweichungen gibt.</p>			
Referenzierte Standards			
<input checked="" type="checkbox"/> BS 10012 <input checked="" type="checkbox"/> ISO/IEC 27001 iVm ISO/IEC 27018			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Zertifizierungsstandards ➔ Prüfungsstandards 			

3.3.4.1.4. Rechtskonforme Datenverarbeitung

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider stellt sicher, dass die Verarbeitung von personenbezogenen Daten unter Einhaltung des geltenden österreichischen und europäischen Datenschutzrechts erfolgt.</p>			
Weiterführende Informationen			
<ul style="list-style-type: none"> ➔ Rechtsvorschriften ➔ Datenschutzrechtliche Orientierungshilfen 			

3.3.4.1.5. Benennung eines zentralen Ansprechpartners

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Der Cloud-Service-Provider benennt eine zentrale Ansprechpartnerin bzw. einen zentralen Ansprech-</p>			

partner (Datenschutzbeauftragte/n), die/der dem Cloud-Service-Kunden für alle Belange des Datenschutzes beim Cloud-Service-Provider und etwaiger weiterer Dienstleister und Subdienstleister zur Verfügung steht und stellt dem Cloud-Service-Kunden deren/dessen Kontaktdaten zur Verfügung, einschl. Name, Telefonnummer und E-Mail-Adresse.

Weiterführende Informationen

- ➔ Rechtsvorschriften
- ➔ Datenschutzrechtliche Orientierungshilfen

3.3.4.1.6. Betroffenenrechte

Schutzbedarf

<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
-------------------------------------	--	--	---

Anforderung

Der Cloud-Service-Provider stellt sicher, dass alle organisatorischen und technischen Voraussetzungen für die fristgerechte Erfüllung der datenschutzrechtlichen Pflichten des Cloud-Service-Kunden i. Z. m. der Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Mitteilung, Datenübertragbarkeit und dem Widerspruch getroffen sind. Der Cloud-Service-Provider überlässt dem Cloud-Service-Kunden alle dafür notwendigen Informationen.

Weiterführende Informationen

- ➔ Rechtsvorschriften
- ➔ Datenschutzrechtliche Orientierungshilfen

3.3.4.1.7. Informationspflicht bei Datenschutzverletzungen

Schutzbedarf

<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
-------------------------------------	--	--	---

Anforderung

Auftretende Datenschutzverletzungen i. Z. m. dem Cloud-Service werden durch den Cloud-Service-Provider einschließlich aller damit im Zusammenhang stehenden Fakten, Auswirkungen und Maßnahmen dokumentiert und unverzüglich an den Cloud-Service-Kunden gemeldet.

Die Dokumentation und Meldung hat alle Informationen zu enthalten, die der Cloud-Service-Kunde zur Erfüllung von datenschutzrechtlichen Meldepflichten benötigt. Dazu zählt insb. eine Beschreibung

- der Art der Datenschutzverletzung, einschl. der Anzahl der betroffenen Kategorien, Personen und Datensätze,
- der wahrscheinlichen Folgen der Datenschutzverletzung,
- der bereits ergriffenen Maßnahmen zur Behebung der Datenschutzverletzung,
- der vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung sowie
- der vorgeschlagenen Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen.

Weiterführende Informationen

- ➔ Rechtsvorschriften
- ➔ Datenschutzrechtliche Orientierungshilfen

3.3.4.2. Datenschutz-Level

3.3.4.2.1. Datenschutz Level Agreement

Schutzbedarf			
<input type="checkbox"/> Unkritisch	<input checked="" type="checkbox"/> Normal	<input checked="" type="checkbox"/> Hoch	<input checked="" type="checkbox"/> Sehr hoch
Anforderung			
<p>Die zugesicherten Datenschutzparameter des Cloud-Services werden in einem schriftlichen Datenschutz Level Agreement (Vereinbarungen zur Auftragsverarbeitung) zwischen Cloud-Service-Provider und Cloud-Service-Kunden vertraglich vereinbart.</p> <p>Dazu zählen insb. folgende Vereinbarungen:</p> <ul style="list-style-type: none">▪ Auftragsverarbeitung<ul style="list-style-type: none">▪ Gegenstand, Dauer, Art und Zweck der Datenverarbeitung▪ Datenarten und Kategorien betroffener Personen▪ Organisatorische und technische Maßnahmen<ul style="list-style-type: none">▪ Umsetzung, Dokumentation und regelmäßige Überprüfung der erforderlichen Maßnahmen durch den Cloud-Service-Provider▪ Bereitstellung erforderlicher Informationen und Nachweise durch den Cloud-Service-Provider hinsichtlich der Einhaltung seiner datenschutzrechtlichen Pflichten und Umsetzung der erforderlichen Maßnahmen auf Anforderung des Cloud-Service-Kunden▪ Standards, Zertifizierungen und Gütesiegel (sofern zutreffend)<ul style="list-style-type: none">▪ Verwendete Datenschutz-Managementsystemstandards▪ Vorhandene Datenschutz-Gütesiegel▪ Vorhandene Datenschutz-Zertifizierungen▪ Kontrollrechte des Cloud-Service-Kunden<ul style="list-style-type: none">▪ Überprüfung des Cloud-Service-Providers durch den Cloud-Service-Kunden hinsichtlich der Einhaltung der Vereinbarungen zur Auftragsverarbeitung bzw. Beauftragung eines Dritten zur Durchführung solcher Überprüfungen▪ Bereitstellung erforderlicher Informationen und Nachweise durch den Cloud-Service-Provider hinsichtlich der Einhaltung seiner datenschutzrechtlichen Pflichten und Umsetzung der erforderlichen organisatorischen und technischen Maßnahmen auf Anforderung des Cloud-Service-Kunden▪ Vertragsverletzungen<ul style="list-style-type: none">▪ Pönale bei Verletzung der vertraglichen Parameter <p>Der Cloud-Service-Provider stellt dem Cloud-Service-Kunden ausführliche Informationen über die getroffenen Maßnahmen zur Sicherstellung des Datenschutzes zur Verfügung.</p>			
Weiterführende Informationen			
<ul style="list-style-type: none">➔ Rechtsvorschriften➔ Datenschutzrechtliche Orientierungshilfen➔ Privacy Level Agreements➔ Rahmenwerke, Handbücher und Kataloge			

3.4. Fazit

Die Auswahl eines geeigneten Cloud-Service-Providers und die Vereinbarung vertraglicher Grundlagen mit diesem sind zentrale Elemente bei der Auslagerung von Daten oder Datenanwendungen in die Cloud. Dabei liegt die größte Herausforderung darin, alle relevanten Aspekte entsprechend zu berücksichtigen. Dieser Abschnitt unterstützt bei dieser Tätigkeit, indem er eine Vielzahl an potenziell relevanten Aspekten in Form repräsentativer Anforderungskriterien definiert.

Dabei erhebt der Cloud Computing Kompass keinen Anspruch auf Vollständigkeit. Um Interessierten bei jenen Inhalten, bei denen der Cloud Computing Kompass in Bezug auf Vollständigkeit und Detailtiefe bewusst gesetzte Grenzen hat, eine weitere Vertiefung in die Materie zu erleichtern, listet der folgende Abschnitt einschlägige weiterführende Dokumente und Informationsquellen auf.

4. Weiterführende Informationen

An Empfehlungen und Standards rund um das Thema Cloud Computing mangelt es nicht. Im Gegenteil – aufgrund der Vielzahl an nationalen und internationalen Organisationen, Leitfäden, Rechtsvorschriften, Konventionen und Standards ist es mittlerweile schwierig geworden, die Übersicht zu behalten. Die nachfolgende Auswahl soll dies etwas erleichtern. Der Fokus liegt dabei auf jenen Dokumenten, die speziell für österreichische Cloud-Service-Kunden von Bedeutung sind.

Da die in diesem Abschnitt gelisteten Dokumente und Informationen ein sehr breites Spektrum abdecken, ermöglicht dieser letzte Abschnitt ein gezieltes Erarbeiten von Detailwissen zu speziellen Teilbereichen, die der Cloud Computing Kompass aufgrund der bewusst gesetzten Grenzen nur überblicksmäßig behandeln konnte.

4.1. Organisationen

A-SIT	Zentrum für sichere Informationstechnologie – Austria www.a-sit.at
AICPA	American Institute of Certified Public Accountants www.aicpa.org
ANSI	American National Standards Institute www.ansi.org
AS	Austrian Standards Institute www.austrian-standards.at
AXELOS	AXELOS www.axelos.com
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. www.bitkom.org
BLSG	Kooperation Bund-Länder-Städte-Gemeinden www.ref.gv.at
BSI	Bundesamt für Sicherheit in der Informationstechnik www.bsi.bund.de
BSI Group	British Standards Institution Group www.bsigroup.com
CENELEC	European Committee for Electrotechnical Standardization www.cenelec.eu
CIS	Center for Internet Security www.cisecurity.org
CSA	Cloud Security Alliance cloudsecurityalliance.org
ENISA	European Union Agency for Network and Information Security www.enisa.europa.eu

EuroCloud Austria	EuroCloud Austria – gemeinnütziger Verein für Förderung von Cloud Computing www.eurocloud.at
IAASB	International Auditing and Assurance Standards Board www.iaasb.org
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V. www.idw.de
IEC	International Electrotechnical Commission www.iec.ch
IEEE	Institute of Electrical and Electronics Engineers www.ieee.org
IETF	Internet Engineering Task Force www.ietf.org
ISACA	Information Systems Audit and Control Association www.isaca.org
ITU-T	Telecommunication Standardization Sector of the International Telecommunications Union www.itu.int
ISO	International Organization for Standardization www.iso.org
NIST	National Institute of Standards and Technology www.nist.gov
OASIS	Organization for the Advancement of Structured Information Standards www.oasis-open.org
OGF	Open Grid Forum www.ogf.org
OpenID	OpenID Foundation openid.net
OWASP	Open Web Application Security Project www.owasp.org
PCI	Payment Card Industry Security Standards Council www.pcisecuritystandards.org
W3C	World Wide Web Consortium http://www.w3.org

4.2. Cloud-Grundlagen

	TCI Reference Architecture v2 CSA 2013
	Security Guidance for Critical Areas of Focus in Cloud Computing v3 CSA 2011
ISO/IEC 17788	Information technology -- Cloud computing -- Overview and vocabulary ISO/IEC 2014
ISO/IEC 17789	Information technology -- Cloud computing -- Reference architecture ISO/IEC 2014

SP 500-292	Cloud Computing Reference Architecture <u>NIST 2011</u>
SP 500-293	US Government Cloud Computing Technology Roadmap <u>NIST 2014</u>
SP 500-299	Cloud Computing Security Reference Architecture <u>NIST (Entwurf)</u>
SP 500-316	Framework for Cloud Usability <u>NIST 2015</u>

4.3. Cloud-Strategie

	Eckpunkte für sicheres Cloud Computing <u>BITKOM 2013</u>
	Leitfaden Cloud Computing – Was Entscheider wissen müssen <u>BITKOM 2010</u>
	Cloud Computing Eckpunktepapier <u>BSI 2012</u>
	Sichere Nutzung von Cloud-Diensten <u>BSI 2016</u>
	Procure Secure <u>ENISA 2012</u>
	Critical Cloud Computing <u>ENISA 2013</u>
	Good Practice Guide for securely deploying Governmental Clouds <u>ENISA 2013</u>
	Security Framework for Governmental Clouds <u>ENISA 2015</u>
SP 500-291	Cloud Computing Standards Roadmap <u>NIST 2011</u>
SP 500-322	Evaluation of Cloud Computing Services <u>NIST (Entwurf)</u>

4.4. Rechtsvorschriften

AktG	Aktiengesetz <u>StF: BGBl. Nr. 98/1965 idF BGBl. Nr. 24/1985</u>
BAO	Bundesabgabenordnung <u>StF: BGBl. Nr. 194/1961</u>
BVergG 2006	Bundesvergabegesetz 2006 <u>StF: BGBl. I Nr. 17/2006</u>
BVergGVS 2012	Bundesvergabegesetz Verteidigung und Sicherheit 2012 <u>StF: BGBl. I Nr. 10/2012</u>
BWG	Bankwesengesetz <u>StF: BGBl. Nr. 532/1993 idF BGBl. Nr. 639/1993</u>

DSG	Datenschutzgesetz StF: BGBl. I Nr. 120/2017
DSG 2000	Datenschutzgesetz 2000 StF: BGBl. I Nr. 165/1999
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG VO (EU) 2016/679
E-GovG	E-Government-Gesetz StF: BGBl. I Nr. 10/2004
eIDAS-VO	Verordnung (EU) Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257/73 vom 28. August 2014 VO (EU) Nr. 910/2014
Genossenschaftsgesetz	Genossenschaftsgesetz StF: RGBl. Nr. 70/1873
GmbHG	GmbH-Gesetz StF: RGBl. Nr. 58/1906
GTelG 2012	Gesundheitstelematikgesetz 2012 StF: BGBl. I Nr. 111/2012
GTelV 2013	Gesundheitstelematikverordnung 2013 StF: BGBl. II Nr. 506/2013
InfoSiG	Informationssicherheitsgesetz StF: BGBl. I Nr. 23/2002
InfoSiV	Informationssicherheitsverordnung StF: BGBl. II Nr. 548/2003
NIS-RL	Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. Nr. L 194 vom 19. Juli 2016 RL (EU) 2016/1148
NISG	Netz- und Informationssystemsicherheitsgesetz Entwurf (noch nicht verfügbar)
SVG	Signatur- und Vertrauensdienstegesetz StF: BGBl. I Nr. 50/2016
SVV	Signatur- und Vertrauensdiensteverordnung StF: BGBl. II Nr. 208/2016
TKG 2003	Telekommunikationsgesetz 2003 StF: BGBl. I Nr. 70/2003
TKG-DSVO	Datensicherheitsverordnung StF: BGBl. II Nr. 402/2011
Urheberrechtsgesetz	Urheberrechtsgesetz StF: BGBl. Nr. 111/1936
VAG 2016	Versicherungsaufsichtsgesetz 2016 StF: BGBl. I Nr. 34/2015

4.5. Datenschutzrechtliche Orientierungshilfen

17/EN WP 248	<p>Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Art. 29 Datenschutzarbeitsgruppe (WP29) der Europäischen Kommission 2017</p> <p>Leitfaden zur Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung DSB 2017</p> <p>Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Deutschland) 2016</p> <p>White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz Forum Privatheit (Deutschland) 2016</p>
GDD-Praxishilfe DS-GVO II	<p>Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung Gesellschaft für Datenschutz und Datensicherheit e.V. (Deutschland) 2016</p>
GDD-Praxishilfe DS-GVO IV	<p>Vertragsmuster zur Auftragsverarbeitung Gesellschaft für Datenschutz und Datensicherheit e.V. (Deutschland) 2017</p>
GDD-Praxishilfe DS-GVO VII	<p>Transparenzpflichten bei der Datenverarbeitung Gesellschaft für Datenschutz und Datensicherheit e.V. (Deutschland) 2017</p>

4.6. E-Government-Konventionen

	<p>Sicherheitsempfehlungen für Behörden - Teil 1: Empfehlungen zur Verwendung kryptographischer Methoden A-SIT 2016</p> <p>Sicherheitsempfehlungen für Behörden - Teil 2: Empfehlungen zur Verwendung von SSL/TLS A-SIT 2016</p>
CommonAuditTrail	<p>Common Audit Trail Exchange Format BLSG 2011 (nur für BLSG-Teilnehmer frei verfügbar)</p>
PVP-AuditQuery	<p>Revisionsabfrage im Portalverbund BLSG 2009 (nur für BLSG-Teilnehmer frei verfügbar)</p>
PVP-SMA	<p>Portalverbund Sicherheitsmaßnahmen BLSG 2016 (nur für BLSG-Teilnehmer frei verfügbar)</p>
SecClass	<p>Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen BLSG 2008 (nur für BLSG-Teilnehmer frei verfügbar)</p>
Sicherheitsstufen	<p>Sicherheitsstufen für die Kommunikation Bürger – Behörde BLSG 2003 (nur für BLSG-Teilnehmer frei verfügbar)</p>
GehSO	<p>Geheimhaltungsordnung des Bundes 2008 (nicht öffentlich verfügbar)</p>

Nationale Kryptostrategie
[ISK 2016](#) (nicht öffentlich verfügbar)

Vorgaben der ISK zu E-Mail für klassifizierte Informationen
[ISK 2016](#) (nicht öffentlich verfügbar)

TLS-Vorgaben der ISK für klassifizierte Informationen
[ISK 2016](#) (nicht öffentlich verfügbar)

4.7. Zertifizierungsstandards

ANSI/TIA 942	Telecommunications Infrastructure Standard for Data Centers ANSI 2012
BS 10012	Data protection - Specification for a personal information management system BSI Group 2017
BSI-ITGS	ISO/IEC 27001 auf Basis des BSI IT-Grundschutzes BSI 2016 (mittlerweile IT-Grundschutz-Kompendium)
EN 50600	Information technology - Data centre facilities and infrastructures CENELEC 2012
ISO/IEC 15408	Information technology -- Security techniques -- Evaluation criteria for IT security ISO/IEC 2009
ISO/IEC 17021-1	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements ISO/IEC 2015
ISO/IEC 17021-2	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 2: Competence requirements for auditing and certification of environmental management systems ISO/IEC 2016
ISO/IEC 17021-3	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 3: Competence requirements for auditing and certification of quality management systems ISO/IEC 2017
ISO/IEC TS 17021-4	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 4: Competence requirements for auditing and certification of event sustainability management systems ISO/IEC 2013
ISO/IEC TS 17021-5	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 5: Competence requirements for auditing and certification of asset management systems ISO/IEC 2014
ISO/IEC TS 17021-6	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 6: Competence requirements for auditing and certification of business continuity management systems ISO/IEC 2014

ISO/IEC TS 17021-7	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 7: Competence requirements for auditing and certification of road traffic safety management systems ISO/IEC 2014
ISO/IEC TS 17021-9	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 9: Competence requirements for auditing and certification of anti-bribery management systems ISO/IEC 2016
ISO/IEC NP 17021-10	Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 10: Competence requirements for auditing and certification of occupational health and safety management systems ISO/IEC Entwurf (noch nicht verfügbar)
ISO 22301	Societal security -- Business continuity management systems -- Requirements ISO 2012
ISO/IEC 20000-1	Information technology -- Service management -- Part 1: Service management system requirements ISO/IEC 2011
ISO/IEC 20000-6	Information technology -- Service management -- Part 6: Requirements for bodies providing audit and certification of service management systems ISO/IEC 2017
ISO/IEC TR 20000-9	Information technology -- Service management -- Part 9: Guidance on the application of ISO/IEC 20000-1 to Cloud-Services ISO/IEC 2015
ISO/IEC 27001	Information technology -- Security techniques -- Information security management systems -- Requirements ISO/IEC 2013
ISO/IEC 27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors ISO/IEC 2014
ÖNORM A-7700	Informationsverarbeitung - Sicherheitstechnische Anforderungen an Webapplikationen AS 2008

4.8. Prüfungsstandards

AT Section 101	Attestation Engagements AICPA 2016
AT Section 801	Reporting on Controls at a Service Organization AICPA 2016
IDW PS 330	IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie IDW 2002

IDW PS 880	IDW Prüfungsstandard: Die Prüfung von Softwareprodukten <u>IDW 2015</u>
IDW PS 951	IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen <u>IDW 2013</u>
ISAE 3000	International Standard on Assurance Engagements (ISAE) No. 3000 Standard for assurance over non-financial information <u>IAASB 2013</u>
ISAE 3402	International Standard on Assurance Engagements (ISAE) No. 3402 Assurance Reports on Controls at a Service Organization <u>IAASB 2010</u>

4.9. Gütesiegel

CSA STAR	CSA Security, Trust & Assurance Registry <u>cloudsecurityalliance.org/star</u>
ESCloud Label	European Secure Cloud Label <u>www.bsi.bund.de</u>
EuroCloud StarAudit	EuroCloud StarAudit <u>staraudit.org</u>
EuroPriSe	Europäisches Datenschutz-Gütesiegel <u>www.european-privacy-seal.eu</u>
Trusted Cloud-Service	TÜV TRUST IT <u>it-tuv.com</u>

4.10. Servicestandards

4.10.1. Anforderungen an Cloud-Services

ISO/IEC TR 20000-9	Information technology -- Service management -- Part 9: Guidance on the application of ISO/IEC 20000-1 to Cloud-Services <u>ISO/IEC 2015</u>
--------------------	---

4.10.2. IT-Servicemanagement

ISO/IEC 20000-1	Information technology -- Service management -- Part 1: Service management system requirements <u>ISO/IEC 2011</u>
ISO/IEC 20000-2	Information technology -- Service management -- Part 2: Guidance on the application of service management systems <u>ISO/IEC 2012</u>
ISO/IEC 20000-3	Information technology -- Service management -- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1 <u>ISO/IEC 2012</u>

ISO/IEC TR 20000-4	Information technology -- Service management -- Part 4: Process reference model ISO/IEC 2010
ISO/IEC TR 20000-5	Information technology -- Service management -- Part 5: Exemplar implementation plan for ISO/IEC 20000-1 ISO/IEC 2013
ISO/IEC TR 20000-10	Information technology -- Service management -- Part 10: Concepts and terminology ISO/IEC 2015
ISO/IEC TR 20000-11	Information technology -- Service management -- Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL ISO/IEC 2015
ISO/IEC TR 20000-12	Information technology -- Service management -- Part 12: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: CMMI-SVC ISO/IEC 2016
ITIL	IT Infrastructure Library V3 AXELOS 2011
COBIT	Control Objectives for Information and Related Technology V5 ISACA 2012

4.10.3. Service Level Agreements

ISO/IEC 19086-1	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts ISO/IEC 2016
ISO/IEC 19086-2	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model ISO/IEC Entwurf
ISO/IEC 19086-3	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 3: Core conformance requirements ISO/IEC Entwurf

4.10.4. Interoperabilität und Portabilität

IEEE P2301	Guide for Cloud Portability and Interoperability Profiles (CPIP) IEEE Entwurf
IEEE P2302	Standard for Intercloud Interoperability and Federation (SIIF) IEEE Entwurf
ISO/IEC 17203	Information technology -- Open Virtualization Format (OVF) specification ISO/IEC 2011
ISO/IEC 17826	Information technology -- Cloud Data Management Interface (CDMI) ISO/IEC 2016
ISO/IEC 19831	Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol -- An Interface for Managing Cloud Infrastructure ISO/IEC 2015

ISO/IEC 19941	Information technology -- Cloud computing -- Interoperability and portability ISO/IEC Entwurf
ISO/IEC 19944	Information technology -- Cloud computing -- Cloud-Services and devices: Data flow, data categories and data use ISO/IEC Entwurf
KMIP	Key Management Interoperability Protocol OASIS
OCCI	Open Cloud Computing Interface (OCCI) Open Grid Forum 2016

4.11. Sicherheitsstandards

4.11.1. Anforderungen an Cloud-Services

BSI-C5	Anforderungskatalog Cloud Computing (C5) - Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten BSI 2016
CSA-CCM	Cloud Controls Matrix (CCM) v3.0.1 CSA 2016
CSA-CAIQ	Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1 CSA 2016
ENISA-IAF	Cloud Computing Information Assurance Framework ENISA 2009
ISO/IEC 27017	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud-Services ISO/IEC 2015
ISO/IEC 27036-4	Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services ISO/IEC 2016
SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing NIST 2011

4.11.2. Informationssicherheitsmanagement

ISHB	Österreichisches Informationssicherheitshandbuch A-SIT 2016
BSI-Standard 100-1	Managementsysteme für Informationssicherheit – ISMS BSI 2008
BSI-Standard 100-2	IT-Grundschutz-Vorgehensweise BSI 2008
BSI-ITGS	IT-Grundschutz-Kataloge BSI 2016 (mittlerweile IT-Grundschutz-Kompodium)

ISO/IEC 27001	Information technology -- Security techniques -- Information security management systems -- Requirements ISO/IEC 2013
ISO/IEC 27002	Information technology -- Security techniques -- Code of practice for information security controls ISO/IEC 2013
ISO/IEC 27014	Information technology -- Security techniques -- Governance of information security ISO/IEC 2013
ISO/IEC 27036-1	Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts ISO/IEC 2014
ISO/IEC 27036-2	Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Requirements ISO/IEC 2014
ISO/IEC 27036-3	Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security ISO/IEC 2013
SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations NIST 2013

4.11.3. Risikomanagement

BSI-Standard 100-3	Risikoanalyse auf der Basis von IT-Grundschutz BSI 2008
ISO/IEC 27005	Information technology -- Security techniques -- Information security risk management ISO/IEC 2011
ISO 31000	Risk management -- Principles and guidelines ISO 2009
IEC 31010	Risk management -- Risk assessment techniques IEC 2009
ONR 49000	Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen AS 2014
ONR 49001	Risikomanagement für Organisationen und Systeme - Risikomanagement AS 2014
ONR 49002-1	Risikomanagement für Organisationen und Systeme - Teil 1: Leitfaden für die Einbettung des Risikomanagements ins Managementsystem AS 2014
ONR 49002-2	Risikomanagement für Organisationen und Systeme - Teil 2: Leitfaden für die Methoden der Risikobeurteilung AS 2014

ONR 49002-3	Risikomanagement für Organisationen und Systeme - Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement AS 2014
ONR 49003	Risikomanagement für Organisationen und Systeme - Anforderungen an die Qualifikation des Risikomanagers AS 2014
SP 800-39	Managing Information Security Risk NIST 2011

4.11.4. Auditierung und Test

ISO 19011	Guidelines for auditing management systems ISO 2011
ISO/IEC 27007	Information technology -- Security techniques -- Guidelines for information security management systems auditing ISO/IEC 2011
ISO/IEC TR 27008	Information technology -- Security techniques -- Guidelines for auditors on information security controls ISO/IEC 2011
SP 800-115	Technical Guide to Information Security Testing and Assessment NIST 2008

4.11.5. Sicherheitsschwachstellenmanagement

X.1500	Overview of cyber security information exchange ITU-T 2011
X.1520	Common vulnerabilities and exposures (CVE) ITU-T 2014
X.1521	Common vulnerability scoring system (CVSS) 3.0 ITU-T 2016
X.1524	Common weakness enumeration (CWE) ITU-T 2012
X.1525	Common weakness scoring system (CWSS) ITU-T 2015
X.1526	Language for the open definition of vulnerabilities and for the assessment of a system state (OVAL) ITU-T 2014
X.1528	Common platform enumeration (CPE) ITU-T 2012
X.1528.1	Common platform enumeration (CPE) naming ITU-T 2012
X.1528.2	Common platform enumeration (CPE) name matching ITU-T 2012
X.1528.3	Common platform enumeration (CPE) dictionary ITU-T 2012
X.1528.4	Common platform enumeration (CPE) applicability language ITU-T 2012

X.1544 Common attack pattern enumeration and classification (CAPEC)
[ITU-T 2013](#)

4.11.6. Sicherheitsvorfallmanagement

	Incident Reporting for Cloud Computing <u>ENISA 2013</u>
ISO/IEC 27035-1	Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management <u>ISO/IEC 2016</u>
ISO/IEC 27035-2	Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response <u>ISO/IEC 2016</u>
ISO/IEC 27037	Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence <u>ISO/IEC 2012</u>
ISO/IEC 27039	Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection and prevention systems (IDPS) <u>ISO/IEC 2015</u>
SP 800-61	Computer Security Incident Handling Guide <u>NIST 2012</u>
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response <u>NIST 2006</u>

4.11.7. Business Continuity Management

BSI-Standard 100-4	Notfallmanagement <u>BSI 2008</u>
ISO 22301	Societal security -- Business continuity management systems -- Requirements <u>ISO 2012</u>
ISO/IEC 27031	Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity <u>ISO/IEC 2011</u>

4.11.8. Applikationssicherheit

ISO/IEC TS 17961	Information technology -- Programming languages, their environments and system software interfaces -- C secure coding rules <u>ISO/IEC 2013</u>
ISO/IEC TR 24731	Information technology -- Programming languages, their environments and system software interfaces -- Extensions to the C library -- Part 1: Bounds-checking interfaces <u>ISO/IEC 2007</u>

ISO/IEC 27034-1	Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts ISO/IEC 2011
ISO/IEC 27034-2	Information technology -- Security techniques -- Application security -- Part 2: Organization normative framework ISO/IEC 2015
ISO/IEC 27034-3	Information technology -- Application security -- Part 3: Application security management process ISO/IEC Entwurf
ISO/IEC 27034-5	Information technology -- Security techniques -- Application security -- Part 5: Protocols and application security controls data structure ISO/IEC Entwurf (noch nicht verfügbar)
ISO/IEC 27034-6	Information technology -- Security techniques -- Application security -- Part 6: Case studies ISO/IEC 2016
ÖNORM A-7700	Informationsverarbeitung - Sicherheitstechnische Anforderungen an Webapplikationen AS 2008
OWASP-AS	Open Web Application Security Project - Application Security OWASP
SP 800-64	Security Considerations in the System Development Life Cycle NIST 2008

4.11.9. Identity- und Access-Management

ISO/IEC 9797-1	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher ISO/IEC 2011 (2016)
ISO/IEC 9797-2	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function ISO/IEC 2011 (2016)
ISO/IEC 9797-3	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-function ISO/IEC 2011 (2017)
ISO/IEC 9798-1	Information technology -- Security techniques -- Entity authentication - - Part 1: General ISO/IEC 2010 (2016)
ISO/IEC 9798-2	Information technology -- Security techniques -- Entity authentication - - Part 2: Mechanisms using symmetric encipherment algorithms ISO/IEC 2008
ISO/IEC 9798-4	Information technology -- Security techniques -- Entity authentication - - Part 4: Mechanisms using a cryptographic check function ISO/IEC 1999 (2016)
ISO/IEC 9798-5	Information technology -- Security techniques -- Entity authentication - - Part 5: Mechanisms using zero-knowledge techniques ISO/IEC 2009 (2015)

ISO/IEC 9798-6	Information technology -- Security techniques -- Entity authentication - - Part 6: Mechanisms using manual data transfer ISO/IEC 2010 (2016)
ISO/IEC 24760-1	Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts ISO/IEC 2011
ISO/IEC 24760-2	Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements ISO/IEC 2015
ISO/IEC 24760-3	Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice ISO/IEC 2016
ISO/IEC 29115	Information technology -- Security techniques -- Entity authentication assurance framework ISO/IEC 2013
ISO/IEC 29191	Information technology -- Security techniques -- Requirements for partially anonymous, partially unlinkable authentication ISO/IEC 2012
RFC 5849	Oauth (Open Authorization Protocol) IETF 2010
FIPS 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors NIST 2013
SAML	Security Assertion Markup Language OASIS
SPML	Service Provisioning Markup Language OASIS
XACML	eXtensible Access Control Markup Language OASIS
OpenID	OpenID Authentication OpenID

4.11.10. Kryptografie

BSI TR-02102-1	Kryptographische Verfahren: Empfehlungen und Schlüssellängen BSI 2017
BSI TR-02102-2	Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 2 – Verwendung von Transport Layer Security (TLS) BSI 2017
BSI TR-02102-3	Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2) BSI 2017
BSI TR-02102-4	Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 4 – Verwendung von Secure Shell (SSH) BSI 2017

ISO/IEC 7064	Information technology -- Security techniques -- Check character systems ISO/IEC 2003
ISO/IEC 9796-2	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms ISO/IEC 2010 (2016)
ISO/IEC 9796-3	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms ISO/IEC 2006 (2013)
ISO/IEC 10116	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher ISO/IEC 2017
ISO/IEC 10118-1	Information technology -- Security techniques -- Hash-functions -- Part 1: General ISO/IEC 2016
ISO/IEC 10118-2	Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher ISO/IEC 2010 (2016)
ISO/IEC 10118-3	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions ISO/IEC 2004 (2013)
ISO/IEC 10118-4	Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic ISO/IEC 1998 (2016)
ISO/IEC 11770-1	Information technology -- Security techniques -- Key management -- Part 1: Framework ISO/IEC 2010 (2016)
ISO/IEC 11770-2	Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques ISO/IEC 2008 (2014)
ISO/IEC 11770-3	Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques ISO/IEC 2015
ISO/IEC 11770-4	Information technology -- Security techniques -- Key management -- Part 4: Mechanisms based on weak secrets ISO/IEC 2006 (2013)
ISO/IEC 11770-5	Information technology -- Security techniques -- Key management -- Part 5: Group key management ISO/IEC 2011 (2017)
ISO/IEC 11770-6	Information technology -- Security techniques -- Key management -- Part 6: Key derivation ISO/IEC 2016
ISO/IEC TR 14516	Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services ISO/IEC 2002 (2013)

ISO/IEC 14888-1	Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General ISO/IEC 2008 (2014)
ISO/IEC 14888-2	Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms ISO/IEC 2008 (2014)
ISO/IEC 14888-3	Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms ISO/IEC 2016
ISO/IEC 15945	Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures ISO/IEC 2002 (2013)
ISO/IEC 15946-1	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General ISO/IEC 2016
ISO/IEC 15946-5	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation ISO/IEC 2009 (2015)
ISO/IEC 18031	Information technology -- Security techniques -- Random bit generation ISO/IEC 2011 (2017)
ISO/IEC 18032	Information technology -- Security techniques -- Prime number generation ISO/IEC 2005 (2011)
ISO/IEC 18033-1	Information technology -- Security techniques -- Encryption algorithms -- Part 1: General ISO/IEC 2015
ISO/IEC 18033-2	Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers ISO/IEC 2006 (2013)
ISO/IEC 18033-3	Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers ISO/IEC 2010 2016
ISO/IEC 18033-4	Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers ISO/IEC 2011 (2017)
ISO/IEC 18033-5	Information technology -- Security techniques -- Encryption algorithms -- Part 5: Identity-based ciphers ISO/IEC 2015
ISO/IEC 18033-6	Information technology -- Encryption algorithms -- Part 6: Homomorphic encryption ISO/IEC Entwurf (noch nicht verfügbar)
ISO/IEC 19772	Information technology -- Security techniques -- Authenticated encryption ISO/IEC 2009 (2014)
ISO/IEC 29192-1	Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General ISO/IEC 2012

ISO/IEC 29192-2	Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers ISO/IEC 2012
ISO/IEC 29192-3	Information technology -- Security techniques -- Lightweight cryptography -- Part 3: Stream ciphers ISO/IEC 2012
ISO/IEC 29192-4	Information technology -- Security techniques -- Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques ISO/IEC 2013
ISO/IEC 29192-5	Information technology -- Security techniques -- Lightweight cryptography -- Part 5: Hash-functions ISO/IEC 2016
ISO/IEC 29192-6	Information technology -- Security techniques -- Lightweight cryptography -- Part 6: Message authentication codes (MACs) ISO/IEC Entwurf (noch nicht verfügbar)
RFC 3820	X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile IETF 2004
RFC 5246	Secure Sockets Layer (SSL) / Transport Layer Security (TLS) IETF 2008
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile IETF 2008
X.509	ISO/IEC 9594-8: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks ITU-T 2016
FIPS 140-2	Security Requirements for Cryptographic Modules NIST 2017
FIPS 180-4	Secure Hash Standard (SHS) NIST 2015
FIPS 186-4	Digital Signature Standard (DSS) NIST 2013
FIPS 197	Advanced Encryption Standard (AES) NIST 2001
FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC) NIST 2008
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions NIST 2015

4.11.11. Systemhärtung

CIS-Benchmarks	Center for Internet Security - Benchmark-Dokumente CIS
OWASP-BSP	Open Web Application Security Project - Backend Security Project OWASP

SP 800-70 Rev. 3	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers NIST 2015
SP 800-126 Rev. 2	Security Content Automation Protocol (SCAP) Revision 2 NIST 2011
SP 800-126 Rev. 3	Security Content Automation Protocol (SCAP) Revision 3 NIST Entwurf
USGCB	United States Government Configuration Baseline NIST

4.11.12. Datenlöschung

ISO/IEC 27040	Information technology -- Security techniques -- Storage security ISO/IEC 2015
SP 800-88	Guidelines for Media Sanitization NIST 2014

4.11.13. Systemevaluierung

ISO/IEC 15408-1	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model ISO/IEC 2009
ISO/IEC 15408-2	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components ISO/IEC 2008
ISO/IEC 15408-3	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components ISO/IEC 2008
ISO/IEC TR 15443-1	Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts ISO/IEC 2012
ISO/IEC TR 15443-2	Information technology -- Security techniques -- Security assurance framework -- Part 2: Analysis ISO/IEC 2012
ISO/IEC TR 15446	Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets ISO/IEC 2009
ISO/IEC 18045	Information technology -- Security techniques -- Methodology for IT security evaluation ISO/IEC 2008
ISO/IEC TR 19791	Information technology -- Security techniques -- Security assessment of operational systems ISO/IEC 2010
ISO/IEC 19790	Information technology -- Security techniques -- Security requirements for cryptographic modules ISO/IEC 2012

ISO/IEC 19792	Information technology -- Security techniques -- Security evaluation of biometrics ISO/IEC 2009
ISO/IEC 21827	Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®) ISO/IEC 2008
ISO/IEC 24759	Information technology -- Security techniques -- Test requirements for cryptographic modules ISO/IEC 2017

4.11.14. Rechenzentren

ANSI/TIA 942	Telecommunications Infrastructure Standard for Data Centers ANSI 2012
EN 50600-1	Information technology - Data centre facilities and infrastructures - Part 1: General concepts CENELEC 2012
EN 50600-2-1	Information technology - Data centre facilities and infrastructures - Part 2-1: Building construction CENELEC 2014
EN 50600-2-2	Information technology - Data centre facilities and infrastructures - Part 2-2: Power distribution CENELEC 2014
EN 50600-2-3	Information technology - Data centre facilities and infrastructures - Part 2-3: Environmental control CENELEC 2014
EN 50600-2-4	Information technology - Data centre facilities and infrastructures - Part 2-4: Telecommunications cabling infrastructure CENELEC 2015
EN 50600-2-5	Information technology - Data centre facilities and infrastructures - Part 2-5: Security systems CENELEC 2016
EN 50600-3-1	Information technology - Data centre facilities and infrastructures - Part 3-1: Management and operational information CENELEC 2016
EN 50600-4-1	Information technology - Data centre facilities and infrastructures - Part 4-1: Overview of and general requirements for key performance indicators CENELEC 2016
EN 50600-4-2	Information technology - Data centre facilities and infrastructures - Part 4-2: Power Usage Effectiveness CENELEC 2017
EN 50600-4-3	Information technology - Data centre facilities and infrastructures - Part 4-3: Renewable Energy Factor CENELEC 2016

4.11.15. Weitere technische Spezifikationen

ISO/IEC 13888-1	Information technology -- Security techniques -- Non-repudiation -- Part 1: General ISO/IEC 2009 (2015)
ISO/IEC 13888-2	Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques ISO/IEC 2010 (2016)
ISO/IEC 13888-3	Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques ISO/IEC 2009 (2015)
ISO/IEC 18014-1	Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework ISO/IEC 2008 (2014)
ISO/IEC 18014-2	Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens ISO/IEC 2009 (2015)
ISO/IEC 18014-3	Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens ISO/IEC 2009 (2015)
ISO/IEC 18014-4	Information technology -- Security techniques -- Time-stamping services -- Part 4: Traceability of time sources ISO/IEC 2015
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems NIST 2004
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems NIST 2006
PCI DSS	PCI Data Security Standard PCI 2016
XMLDSig	XML signature W3C 2008
XMLESP	XML Encryption Syntax and Processing W3C 2013

4.12. Datenschutzstandards

4.12.1. Anforderungen an Cloud-Services

ISO/IEC 27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors ISO/IEC 2014
---------------	---

4.12.2. Datenschutzmanagement

BS 10012	Data protection - Specification for a personal information management system BSI Group 2017
----------	--

4.12.3. Datenschutzfolgenabschätzung

ISO/IEC 29134	Information technology -- Security techniques -- Guidelines for privacy impact assessment ISO/IEC 2017
---------------	---

4.12.4. Privacy Level Agreements

CSA PLA v2	Privacy Level Agreement v2 CSA 2015
------------	--

4.12.5. Rahmenwerke, Handbücher und Kataloge

ISO/IEC 19608	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 ISO/IEC Entwurf
ISO/IEC 20889	Information technology -- Security techniques -- Privacy enhancing data de-identification techniques ISO/IEC Entwurf
ISO/IEC 24745	Information technology -- Security techniques -- Biometric information protection ISO/IEC 2011
ISO/IEC 29100	Information technology -- Security techniques -- Privacy framework ISO/IEC 2011
ISO/IEC 29101	Information technology -- Security techniques -- Privacy architecture framework ISO/IEC 2013
ISO/IEC 29151	Information technology -- Security techniques -- Code of practice for personally identifiable information protection ISO/IEC Entwurf
ISO/IEC 29190	Information technology -- Security techniques -- Privacy capability assessment model ISO/IEC 2015
SP 800-53 Appendix J	Privacy Control Catalog NIST 2013
SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) NIST 2010

4.13. Fazit

Bei der Auslagerung von Daten oder Datenanwendungen in die Cloud sind eine Reihe technischer, organisatorischer und rechtlicher Aspekte zu beachten. Dazu zählen unter anderem Rechtsvorschriften, Konventionen, Gütesiegel und auch Prüfungs-, Service-, Sicherheits- und Datenschutzstandards. Für jede dieser Kategorien gibt es eine Vielzahl an Dokumenten, die je nach gegebenem Anwendungsfall von Bedeutung sein können.

Die Vielzahl potenziell relevanter Dokumente macht es schwierig, hier einen Überblick zu behalten. Folgend seinem Bestimmungszweck dient der Cloud Computing Kompass hier als Orientierungshilfe und erleichtert das Auffinden von und Navigieren durch relevante Dokumente, indem diese in diesem letzten Abschnitt gelistet und kategorisiert wurden. Damit fungiert der Cloud Computing Kompass als Einstiegspunkt für eine weitere zielgerichtete Vertiefung in die Materie des Cloud Computing.

Abkürzungsverzeichnis

A

A-SIT	Zentrum für sichere Informationstechnologie – Austria
Abs.	Absatz
AES	Advanced Encryption Standard
AICPA	American Institute of Certified Public Accountants
AktG	Aktiengesetz
ANSI	American National Standards Institute
Art.	Artikel
API	Application Programming Interface
AS	Austrian Standards Institute
ASCII	American Standard Code for Information Interchange
AT	Österreich

B

BAO	Bundesabgabenordnung
BBG	Bundesbeschaffung GmbH
BGBI	Bundesgesetzblatt
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BLSG	Kooperation Bund-Länder-Städte-Gemeinden
BS	British Standards
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSP	Backend Security Project
BVergG 2006	Bundesvergabegesetz 2006
BVergGVS 2012	Bundesvergabegesetz Verteidigung und Sicherheit 2012
BVwG-EV	BVwG-elektronischer-Verkehr-Verordnung
BWG	Bankwesengesetz
bzw.	beziehungsweise

C

CAIQ	Consensus Assessments Initiative Questionnaire
CAPEC	Common attack pattern enumeration and classification
CCM	Cloud Controls Matrix
CDMI	Cloud Data Management Interface
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CIMI	Cloud Infrastructure Management Interface
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPE	Common platform enumeration
CPIP	Cloud Portability and Interoperability Profiles
CRL	Certificate Revocation List
CSA	Cloud Security Alliance
CSS	Cascading Style Sheets
CSV	Comma-separated values
CVE	Common vulnerabilities and exposures
CVSS	Common Vulnerability Scoring System
CWE	Common weakness enumeration
CWSS	Common weakness scoring system

D

DE	Deutschland
DoS	Denial of Service
DS	Datenschutz
DSB	Datenschutzbehörde
DSFA	Datenschutzfolgenabschätzung
DSG	Datenschutzgesetz
DSG 2000	Datenschutzgesetz 2000
DSGVO	Datenschutz-Grundverordnung
DSS	Digital Signature Standard

E

E-GovG	E-Government-Gesetz
EDIAKT	Kommunikationsschnittstelle für elektronische Akten
EDIDOC	Kommunikationsformat für elektronische Akten
eIDAS-VO	Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
einschl.	einschließlich
EN	Europäische Norm
ENISA	European Union Agency for Network and Information Security
etc.	et cetera
EU	Europäische Union

F

FIPS	Federal Information Processing Standard
------	---

G

GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
GehSO	Geheimhaltungsordnung des Bundes
gem.	gemäß
GIF	Graphics Interchange Format
GmbHG	GmbH-Gesetz
GTelG 2012	Gesundheitstelematikgesetz 2012
GTelV 2013	Gesundheitstelematikverordnung 2013

H

HMAC	Keyed-Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol

I

i. d. R.	in der Regel
IaaS	Infrastructure as a Service
IAASB	International Auditing and Assurance Standards Board
ID	Identity
IDC	International Data Corporation
IDPS	Intrusion Detection and Prevention Systems
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKS	internes Kontrollsystems
InfoSiG	Informationssicherheitsgesetz

InfoSiV	Informationssicherheitsverordnung
insb.	insbesondere
INT	international
IPsec	Internet Protocol Security
IS	Informationssicherheit
ISAE	International Standards for Assurance Engagements
ISK	Informationssicherheitskommission
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	IT Infrastructure Library
ITSM	IT-Service-Management
ITU-T	Telecommunication Standardization Sector of the International Telecommunications Union
i. Z. m.	im Zusammenhang mit
J	
JPEG	Joint Photographic Experts Group
L	
LDAP	Lightweight Directory Access Protocol
M	
MTPD	Maximum tolerable period of disruption
MAC	Message Authentication Code
N	
n. F.	neue Fassung
NIS-RL	EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
NISG	Netz- und Informationssystemssicherheitsgesetz
NIST	National Institute of Standards and Technology
O	
OASIS	Organization for the Advancement of Structured Information Standards
OCCI	Open Cloud Computing Interface
OGF	Open Grid Forum
ÖNORM	vom Austrian Standards Institute veröffentlichte nationale Norm
ONR	vom Austrian Standards Institute veröffentlichte Regel
OpenID	OpenID Foundation
OVAL	Language for the open definition of vulnerabilities and for the assessment of a system state
OVF	Open Virtualization Format
OWASP	Open Web Application Security Project
P	
PaaS	Platform as a Service
PCI	Payment Card Industry Security Standards Council
PDF	Portable Document Format
PII	Personally Identifiable Information
PIN	Persönliche Identifikationsnummer
PIV	Personal Identity Verification
PKCS	Public-Key Cryptography Standards
PKI	Public-Key-Infrastructure

PNG	Portable Network Graphics
PS	Prüfungsstandard
PVP	Portalverbundprotokoll
R	
REST	Representational State Transfer
RMS	Risikomanagementsystem
RPO	Recovery Point Objective
RTF	Rich Text Format
RTO	Recovery Time Objective
S	
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SCAP	Security Content Automation Protocol
SDLC	Systems Development Life Cycle
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIIF	Standard for Intercloud Interoperability and Federation
SMS	Short Message Service
SLA	Service Level Agreement
SOA	Service-orientierte Architektur
SOX	Sarbanes-Oxley Act
SP	Special Publication
SPG	Sicherheitspolizeigesetz
SPML	Service Provisioning Markup Language
SSE-CMM	Systems Security Engineering -- Capability Maturity Model
SSH	Secure Shell
SSL	Secure Sockets Layer
StF	Standardfassung
StGB	Strafgesetzbuch
SVG	Signatur- und Vertrauensdienstegesetz
SV	Signatur- und Vertrauensdiensteverordnung
T	
TAN	Transaktionsnummer
TIA	Telecommunications Industry Association
TIFF	Tagged Image File Format
TKG 2003	Telekommunikationsgesetz 2003
TKG-DSVO	Datensicherheitsverordnung
TLS	Transport Layer Security
TR	Technische Richtlinie
U	
UK	United Kingdom
USA	United States of America
USGCB	United States Government Configuration Baseline
V	
VAG 2016	Versicherungsaufsichtsgesetz 2016
W	
W3C	World Wide Web Consortium
WP29	Art. 29 Arbeitsgruppe

WS	Web Services
X	
XACML	eXtensible Access Control Markup Language
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language
XMLDSig	XML signature
XMLESP	XML Encryption Syntax and Processing
Z	
Z	Ziffer
z. B.	zum Beispiel

Impressum

Herausgeber

A-SIT Plus GmbH
Seidlgasse 22/9
A-1030 Wien
office@a-sit.at
www.a-sit.at

Inhalte und Redaktion

A-SIT Plus GmbH und Bundesministerium für Finanzen

Titelbild

Colourbox.de

Stand

Version 1.0
Dezember 2017

In dieser Publikation werden, soweit dies ohne Beeinträchtigung der inhaltlichen Verständlichkeit möglich ist, auch die weiblichen Formen genannt. Es wird jedoch ausdrücklich darauf hingewiesen, dass alle nur in der männlichen Form niedergeschriebenen Formulierungen selbstverständlich auch Frauen gegenüber gelten.

Diese Publikation stellt eine allgemeine und unverbindliche Information dar. Die Inhalte spiegeln die Auffassung der A-SIT Plus GmbH und des Bundesministeriums für Finanzen zum Zeitpunkt der Veröffentlichung wider. Obwohl die Inhalte mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf Richtigkeit, Aktualität und Vollständigkeit. Insbesondere können sie nicht den besonderen Umständen des Einzelfalls Rechnung tragen. Die Publikation kann eine detaillierte Auseinandersetzung mit Rechtsvorschriften und Sicherheitsstandards oder eine umfassende Rechts- und Sicherheitsberatung nicht ersetzen. Eine Verwendung liegt daher in der eigenen Verantwortung der Leserinnen und Leser. Jegliche Haftung wird ausgeschlossen.

Das Projekt SECCAT – Kriterienkatalog, Gütesiegel und Plattform für die Cloud-Sicherheit – wurde von folgendem Konsortium durchgeführt:

IDC Central Europe GmbH

EuroCloud.Austria – Verein zur Förderung von Cloud Computing

REPUCO Unternehmensberatung GmbH

A-SIT Plus GmbH

Bundesministerium für Finanzen



Finanziert im Sicherheitsforschungs-Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie. Projektnummer: 854789.

www.kiras.at | www.bmvit.gv.at

