

Titel des einzuführenden Systems		Hier den Namen der Anwendung eintragen unter der sie auch im Verzeichnisse geführt wird.		
Verantwortliche Stelle		Hier den Namen des Ansprechpartners eintragen.		
Sicherheitsmanagement (Information Security Management - ISM)		ja	nein	Ausführungen / Bemerkungen
ISM-01	Der Cloud-Service-Anbieter hat ein anerkanntes (z. B. nach BSI Standard 100-2 zur Vorgehensweise im IT-Grundschutz oder ISO 27001 / 2) Informationssicherheits-Management-System etabliert und implementiert.			
ISM-02	Das Informationssicherheits-Management-System setzt eine klare Trennung von Aufgaben (Zuständigkeiten), Rollen und Verantwortlichkeiten durch (separation of duties) und benennt dem Cloud-Service-Abonnenten Ansprechpartner für Sicherheitsfragen.			
ISM-03	Der Cloud-Service-Anbieter hat ein zuverlässiges Risikomanagement etabliert, das in regelmäßigen Abständen Bedrohungs- und Risikoanalysen für Daten, Anwendungen, virtuelle und physikalische Ressourcen durchführt. Die Ergebnisse werden dokumentiert, vor Verlust und Manipulation geschützt und dem Cloud-Service-Abonnenten auf Anforderung zur Kenntnis gebracht			
ISM-04	Sicherheitsrichtlinien, Sicherheitsarchitektur und Sicherheitsmaßnahmen des Service werden regelmäßig auf ihre Umsetzung und Wirksamkeit überprüft. Eine Überprüfung kann auf Verlangen des Cloud-Service-Abonnenten auch durch zertifizierte externe Auditoren durchgeführt werden. Die Überprüfung wird dokumentiert. Die Prüfprotokolle und Auditberichte werden vor Verlust und Manipulation geschützt und auf Verlangen dem Cloud-Service-Abonnenten vorgelegt.			
Sicherheitsarchitektur		ja	nein	Ausführungen / Bemerkungen
Rechenzentrumssicherheit (Information Facility Security - IFS)				
IFS-01	Der Zutritt zu Betriebsräumen des Cloud-Service-Anbieters ist nur sicher und zuverlässig authentisierten und autorisierten Personen möglich.			
IFS-02	Der Cloud-Service-Anbieter hat eine robuste und redundante Infrastruktur für die Bereitstellung des Services etabliert, die die Verfügbarkeit der Anwendung auch im Falle von Störungen, Ausfall einzelner Komponenten und beherrschbarer Elementarschäden sicherstellt.			
Sicherheit der Anwendung und der Anwendungsumgebung (Application and Environment Security - AES)				
AES-01	Die Anwendung wird in einer sicheren Betriebsumgebung ausgeführt und stellt die Korrektheit und Integrität importierter und exportierter Daten sicher. Eine Kompromittierung von Daten beim Import oder Export wird zuverlässig verhindert.			
AES-02	Die für den Betrieb erforderliche virtuelle und physikalische Anwendungsumgebung, auf der die Anwendung ausgeführt wird, ist (a) frei von Schadsoftware und Viren, (b) ausreichend gegen interne oder externe netzbasierte Angriffe geschützt und (c) sicher segmentiert (isoliert), so dass eine Eskalation von Zugriffsrechten über die operative Einsatzumgebung ausgeschlossen werden kann. Ein unbefugter und nicht autorisierter Zugriff auf Daten der Anwendung über die operative Einsatzumgebung ist nicht möglich. In der Anwendungsumgebung sind geeignete Werkzeuge installiert, die zuverlässig imstande sind, das Eindringen und die Ausführung von Schadsoftware, Host- bzw. netzbasierte Angriffe zu entdecken und zu verhindern.			
AES-03	Die Anwendung setzt eine sichere Identifikation und Authentisierung externer Zugriffe durch. Ein Zugriff auf Informationen oder Daten der Anwendung ist nur für zuverlässig und sicher authentifizierte und autorisierte Nutzer oder andere Anwendungen oder Services möglich. Unbefugte Zugriffsversuche auf die Anwendung oder Anwendungsdaten bleiben nicht unentdeckt.			
AES-04	Mandanten und Anwendungen und die ihnen zugewiesenen virtuellen und physikalischen Ressourcen (Netze, Server, Speicher) sind sicher segmentiert und isoliert.			
AES-05	Die Anwendung ist so in die Anwendungsumgebung integriert, dass eine Umgehung von der Anwendungsumgebung bereitgestellter Sicherungsmaßnahmen nicht stattfinden kann.			
AES-06	Verbindungen zwischen logischen oder auch physisch voneinander getrennten Komponenten kommen erst nach einer sicheren wechselseitigen Authentisierung zustande. Die Identifikation und Authentisierung wird durch zuverlässige und eindeutige Sicherheitsattribute durchgesetzt. Ein unentdeckter Austausch von Sicherheitskomponenten des Service ist nicht möglich.			
AES-07	Die Anwendung und die Anwendungsumgebung wird auf der Grundlage ausführlicher Richtlinien und Handlungsanweisungen sicher konfiguriert und betrieben. Ein unbefugter Zugriff auf Daten, die für die Konfiguration und den Betrieb der Anwendungsumgebung erforderlich sind, ist nicht möglich.			

AES-08	Konfigurationsänderungen oder Updates werden nur von erfahrenen und ausdrücklich autorisierten Mitarbeitern des Cloud-Service-Anbieters durchgeführt und werden (a) kontrolliert und dokumentiert und (b) vor Inbetriebsetzung auf Sicherheitsbedrohungen getestet. Die Tests werden ausführlich protokolliert, die Testprotokolle vor Verlust oder die Manipulation geschützt.			
AES-09	Sicherheitslücken der Anwendung oder Anwendungsumgebung werden unverzüglich geschlossen und vorhandene Sicherheitspatches unverzüglich implementiert.			
AES-10	Der Cloud-Service-Anbieter etabliert und implementiert sichere Prozesse für die Administration und Wartung der Anwendung und Anwendungs-umgebung. Administration und Wartungsmaßnahmen dürfen nur von vertrauenswürdigen, erfahrenen und ausdrücklich autorisierten Mitarbeitern ausgeführt werden. Für die Administration und Wartung der Anwendung und der Anwendungsumgebung stehen Dokumentationen, Richtlinien oder Handreichungen zur Verfügung, die von den Administratoren und dem Wartungspersonal strikt befolgt werden. Die Maßnahmen werden ausführlich zu protokolliert und die Protokolle vor Verlust und Manipulation geschützt.			
AES-11	Der Cloud-Service-Anbieter hat sichere Prozesse für die Überwachung des Softwarelebenszyklus der Anwendung etabliert und implementiert. Neue Releases werden erst eingesetzt, wenn sie qualitätsgesichert und ausführlichen Sicherheitstests unterzogen wurden.			
AES-12	Der Cloud-Service-Anbieter garantiert die Einhaltung von Sicherheits-Mindeststandards bei der Entwicklung und Bereitstellung von Web-Anwendungen (beispielsweise gemäß den Prinzipien zur sicheren Softwareentwicklung nach OWASP)			
Netzicherheit (Network Security - NCS)		ja	nein	Ausführungen
NCS-01	Netzarchitekturen sind so entworfen, implementiert und konfiguriert, dass Verbindungen zwischen sicheren und unsicheren Netzen nicht möglich sind. Telekommunikations- und Netzverbindungen für den Datentransport, die Kommunikation zwischen logisch oder physisch separierten Komponenten oder Ressourcen und den Servicesupport sind vor Abhören, Manipulation und Zerstörung geschützt. Virtualisierte Netzwerkkomponenten (Verbindungen, Router und Switches) sind zuverlässig und sicher segmentiert und isoliert.			
NCS-02	Der Cloud-Service-Anbieter stellt auf der Grundlage ausführlicher Richtlinien und Handlungsanweisungen die sichere Konfiguration und Segmentierung von Netzkomponenten sicher. Management-Netze (Management-Interfaces) sind strikt von Datennetzen getrennt			
NCS-03	Die Fernadministration des Service erfolgt über einen sicheren Kommunikationskanal (z. B. SSH, IPSec, TLS/SSL, VPN). Der Ausfall oder die Kompromittierung von Management-Netzen (Management-Interfaces) wird zuverlässig verhindert.			
NCS-04	Die Konfiguration der Netzkomponenten wird nur von erfahrenen und ausdrücklich autorisierten Mitarbeitern des Cloud-Service-Anbieters ausgeführt. Änderungen an der Konfiguration von Netzkomponenten werden vor Inbetriebnahme ausführlichen Sicherheitstests unterzogen. Die Tests werden protokolliert, die Protokolle vor Verlust oder Manipulation geschützt.			
NCS-05	Im Falle verteilter Cloud-Computing-Ressourcen sind die Netzverbindungen zwischen den Rechen- oder Datenzentren redundant ausgelegt.			
Datenschutz und Datensicherheit (Data Safety and Security - DSS)		ja	nein	Ausführungen
DSS-01	Der Cloud-Service-Anbieter gewährleistet die Einhaltung der für den Cloud-Service-Abonnenten geltenden datenschutzrechtlichen Regelungen.			
DSS-02	Daten des Cloud-Service-Abonnenten werden außerhalb der am Standort geltenden Gerichtsbarkeit nur mit ausdrücklicher, schriftlicher Zustimmung des Cloud-Service-Abonnenten erfasst, verarbeitet und gespeichert. Das betrifft auch die Verarbeitung und Speicherung von Daten des Cloud-Service-Abonnenten durch Sub-Dienstleister des Cloud-Service-Anbieters.			
DSS-03	Personenbezogene Daten des Cloud-Service-Abonnenten sind - nach Maßgabe zu erwartender Bedrohungen - unter keinen Umständen unbefugten Dritten zugänglich.			
DSS-04	Administratoren, Wartungspersonal oder andere Mitarbeiter des Cloud-Service-Anbieters sowie seines Sub-Dienstleisters haben keinen Zugriff auf geschäftsbezogene Daten des Cloud-Service-Abonnenten.			
DSS-05	Ein unwiederbringlicher Verlust oder ein Diebstahl von Daten des Cloud-Service-Abonnenten wird durch geeignete Sicherheitsmaßnahmen zuverlässig verhindert.			
DSS-06	Der Cloud-Service-Anbieter gewährleistet eine regelmäßige, transparente und redundante Sicherung von Anwendungs- und anwendungsbezogenen Daten.			
DSS-07	Datenträger, auf denen Daten und Informationen des Cloud-Service-Abonnenten aufbewahrt werden, werden regelmäßig auf korrekte Funktion geprüft sowie vor Verlust und Zugriff unbefugter Dritter geschützt.			
DSS-08	Der Cloud-Service-Anbieter stellt die vollständige und nicht wiederherstellbare Löschung von Daten des Cloud-Service-Abonnenten bei Vertragsende oder auf Anforderung des Cloud-Service-Abonnenten sicher.			
Verschlüsselung und Schlüsselmanagement (Public Key Infrastructure - PKI)		ja	nein	Ausführungen

PKI-01	Die Kommunikation zwischen Cloud-Service-Anbieter und Cloud-Service-Abonnenten, Cloud-Computing Standorten sowie Drittdienstleistern erfolgt verschlüsselt.			
PKI-02	Der Cloud-Service-Anbieter stellt ausreichend starke und standardisierte kryptografische Sicherheitsmaßnahmen und Services zur Verfügung, mit denen (a) eine unbefugte Kenntnisnahme oder Manipulation von Daten, Anwendungen, Komponenten und Services verhindert werden kann und (b) die Korrektheit, die Integrität und Authentizität importierter und exportierter Daten zuverlässig gewährleistet wird und eine mögliche Aufdeckung oder Kompromittierung beim Import und Export verhindert werden kann.			
ID- und Rechtemanagement (ID and Rights Management - IDM)		ja	nein	Ausführungen
IDM-01	Der Cloud-Service-Anbieter stellt sicher, dass Zugriffe auf die Anwendung und Anwendungsumgebung nur auf der Basis eines sicheren Identitätsmanagements, Rollen- und Rechtekonzepts, einer starken Authentisierung und einer strikten Trennung von Aufgaben und Zuständigkeiten (separation of duties) erfolgen können.			
IDM-02	Die Umsetzung und Einhaltung des Identitätsmanagements und die Wirksamkeit der implementierten Maßnahmen werden regelmäßig überprüft.			
IDM-03	Ein Diebstahl oder die Fälschung von Identitäten oder Zugriffsrechten wird, mit Blick auf erwartbare Bedrohungsszenarien, zuverlässig verhindert.			
IDM-04	Mitarbeiter erhalten Zugriff nur auf die Funktionen, die sie für die Erfüllung ihrer Aufgaben (ihrer Rolle) benötigen (least privilege).			
IDM-06	Die Zugriffe werden protokolliert. Die Protokolle werden vor Verlust und Manipulation geschützt.			
Kontrollmöglichkeiten für den Nutzer (User Information Control - UIC)		ja	nein	Ausführungen
UIC-01	Die Verfügbarkeit der Anwendung, die Performance und die Auslastung werden ausreichend und transparent protokolliert. Die Protokolle sind vor Verlust und Manipulation geschützt.			
UIC-02	Der Cloud-Service-Abonnent hat die Möglichkeit, Monitoringinformationen hinsichtlich der Verfügbarkeit, Performance und Auslastung über definierte Schnittstellen regelmäßig abzufragen.			
Monitoring und Security Incident Management (SIM)		ja	nein	Ausführungen
SIM-01	Der Cloud-Service-Anbieter hat ein zuverlässiges Monitoring für das Konfigurationsmanagement etabliert und implementiert. Diesbezügliche Aktivitäten von Administratoren werden überwacht und protokolliert. Die Protokolle werden vor Verlust und Manipulation geschützt.			
SIM-02	Der Cloud-Service-Anbieter verfügt über klare Richtlinien sowie etablierte und bewährte Prozesse für die Behandlung sicherheitskritischer Ereignisse.			
SIM-03	Der Cloud-Service-Anbieter stellt die kontinuierliche (24/7) Erkennung, Identifikation und eine unverzügliche und angemessene Behandlung (Einleitung von Gegenmaßnahmen) sicherheitskritischer Ereignisse (security impacts) durch ein erfahrenes und handlungsfähiges Team und geeignete technische Maßnahmen sicher.			
SIM-04	Sicherheitskritische Ereignisse werden dem Cloud-Service-Abonnenten zur Kenntnis gebracht sowie umfassend, ausführlich und transparent dokumentiert. Die Dokumentation wird vor Verlust und Manipulation geschützt und auf Verlangen dem Cloud-Service-Abonnenten vorgelegt.			
Notfallmanagement (Business Continuity Management - BCM)		ja	nein	Ausführungen
BCM-01	Der Cloud-Service-Anbieter hat ein zuverlässiges und sicheres Notfallmanagement etabliert und implementiert. Die darin definierten Maßnahmen und Prozesse werden regelmäßig auf ihre Funktion und Wirksamkeit überprüft. Der Cloud-Service-Anbieter sollte nachweisen, dass sein Notfallmanagement auf international anerkannten Standards wie z. B. BS 25999 (heute ISO 22301) oder BSI-Standard 100-4 basiert (z. B. anhand Notfallvorsorgekonzept und Notfallhandbuch).			
BCM-02	Eine Störung oder ein Ausfall der Verfügbarkeit wird durch eine redundante Auslegung und dynamische Bereitstellung zusätzlicher Instanzen sowie virtueller und physischer Ressourcen verhindert.			
BCM-03	Die Anwendung kann bei einem Systemfehler oder einem erfolgreichen Angriff wieder in einen sicheren und stabilen Zustand zurückgeführt werden.			
BCM-04	Störungen der Verfügbarkeit, die Maßnahmen zur Wiederherstellung und die Zeitdauer der Störung werden zuverlässig und transparent protokolliert, die Protokolle vor Verlust und Manipulation geschützt.			
Sicherheitsüberprüfung und -nachweis (Security Compliance Management - SCM)		ja	nein	Ausführungen
SCM-01	Der Cloud-Service-Anbieter führt regelmäßige Sicherheitsrevisionen/Audits (Überprüfung von Sicherheitskonzepten, Sicherheitsrichtlinien, Sicherheitsarchitekturen und Sicherheitsmaßnahmen, Erkennung und Behandlung sicherheitskritischer Ereignisse) auf der Basis international oder national anerkannter und akzeptierter Standards durch. Das gilt auch für die von ihm vertraglich für die Erstellung des Service gebundenen Sub-Dienstleister.			