ALLIANZ DIGITALE SICHERHEIT SCHWEIZ

Version 3.0 | 01.03.2026

CyberSeal - Prüfliste

Kap.	Pt.	Kontrolle	Prio	Audit- methode: S=Selbst-deklaration I=Interview K=Konsole
5.1		**Aufgabeteilung Kunde/IT-Dienstleister**		
	1	Es besteht eine schriftliche Abmachung über eine Aufgabenteilung mit allen Kunden (z.B. ein SLA, Wartungsvertrag, Servicedescription).	1	I
	2	Es gibt eine für Cybersicherheit verantwortliche Person/Rolle.	1	I
	3	Der IT-Dienstleister erstattet dem Kunden gegenüber ein regelmässiges Security-Reporting.	2	I
5.2		**Verwaltung des Zugriffs auf Kundeninfrastruktur**		
	1	Personalmutationen beim IT-Dienstleister können einfach umgesetzt werden. Ein ehemaliger Mitarbeiter kann nicht mehr auf die Kundeninfrastruktur/-daten zugreifen.	1	I
	2	Der Kunde kann ausschliesslich auf ihm zur Verfügung gestellte Ressourcen beim IT-Dienstleister zugreifen, die Ressourcen anderer Kunden sind gesperrt.	1	I
	3	Der Zugriff auf die Kundeninfrastruktur ist nur mit verwalteten Geräten möglich. Jumphosts und virtuelle Rechner gelten als verwaltet.	1	I
	4	Alle Kunden sind informiert über den Umfang der Berechtigungen des IT-Dienstleisters. (z.B. AGB, SLA)	1	I
	5	Für den Zugriff auf die Kundeninfrastruktur ist eine Mehrfaktor-Authentifizierung notwendig.	1	I
5.3		**Credentials und Berechtigungen**		
	1	Jede Mutation der Accounts (inkl. der Passwörter) oder der Berechtigungen ist nachvollziehbar.	1	S
	2	Die Passwörter des Kunden sind stark, einmalig und sicher verwahrt (Passwortsafe oder ähnliches).	1	S
	3	In einem Notfall (z.B. Ausfall der IT Infrastruktur) sind die Passwörter zugänglich.	1	S
	4	Privilegierte Accounts müssen besonders stark abgesichert sein.	1	S
	5	Es existiert ein definierter und sicherer Prozess für die Mutation der Accounts, des Passwortes und der Berechtigungen.	2	S
	6	Es existiert ein definierter und sicherer Prozess für die Vergabe und den Entzug temporärer Berechtigungen. (z.B. zeitliche Begrenzung)	2	S
5.4		**Dokumentation**		
	1	Für jeden Kunden besteht eine Übersichtsdokumentation mit mindestens Hostname, IP-Adresse und Zweck der verwalteten Komponenten (Inventar).	1	I
	2	Die Dokumentation kann dem Kunden auf Antrag abgegeben werden (allgemein verbreitetes elektronisches Format wie PDF oder Papier).	1	I
	3	Die Dokumentation ist aktuell (nicht älter als 1 Monat nach der letzten Änderung).	2	I
5.5		**Netzwerkdesign**		
	1	Das Netzwerk ist segmentiert: z.B. Office Netzwerk, Core-Komponenten (Storage, Virtualisierungsplattform, Netzwerkkomponenten), Netzwerk in der Produktion, WLAN, Gäste-WLAN.	1	S
	2	Nicht patchbare Systeme/Applikationen müssen in einem separierten Netzwerk betrieben werden.	1	S
	3	Die Übergänge zwischen den Zonen haben minimale Connectivity (z.B. mittels Firewalls).	2	S
5.6		**Firewalls**		
	1	Die Regeln müssen lesbar sein (sinnvolle, mit Dokumentation übereinstimmende Bezeichnungen). Dokumentationen im Ruleset sind erwünscht.	1	I
	2	Das Ruleset muss regelmässig und nachvollziehbar überprüft werden. Ein Vieraugenprinzip wird empfohlen.	1	I
	3	Das Ruleset ist möglichst eng definiert. Z.B. sind Any-Any-Regeln nicht erlaubt, auch ausgehender Verkehr ist eingeschränkt. Ausnahmen sind zu begründen.	2	I
5.7		**WLAN**		
	1	Für jeden Kunden müssen separate, nicht ableitbare Passwörter verwendet werden.	1	I
	2	Es muss ein separates WLAN für private Geräte von Mitarbeitern und für Gäste eingerichtet werden.	1	I
	3	Es werden ausschliesslich aktuelle und sichere Schutzmechanismen verwendet.	2	I
5.8		**Identity Management (Active Directory, Azure, ...)**		
	1	Der Kunde besitzt einen Notfall-Administrator-Account, ausser er verzichtet explizit darauf.	1	S
	2	Accounts mit erweiterten Berechtigungen werden nicht für die täglichen Anwendungsarbeiten verwendet.	1	S
	3	Öffentlich zugreifbare Portale (z.B. Azure), welche mit dem eigenen AD synchronisiert sind, werden mit Mehrfaktor-Authentifizierung geschützt.	1	S
	4	Der IT-Dienstleister hat pro Kunde einen eigenen Administrator-Account mit unterschiedlichen Credentials.	2	S
	5	Die Identitäten und Berechtigungen müssen regelmässig überprüft werden (zumindest jährlich).	2	S
5.9		**Hardening der IT-Komponenten**		
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für die Härtung der Systeme (Clients, Server, Netzwerk-Komponenten etc.).	1	I
5.10		**Mail-System**		
	1	Der IT-Dienstleister stellt sicher, dass die E-Mail-Infrastrukturen vor Malware und Spam geschützt sind.	1	K
	2	Der IT-Dienstleister unterstützt nur E-Mail-Infrastrukturen, die die Absenderauthentizität prüfen (SPF, DKIM etc.).	1	K

Version 3.0 | 01.03.2026

CyberSeal - Prüfliste

Kap.	Pt.	Kontrolle	Prio	Audit- methode: S=Selbst-deklaration I=Interview K=Konsole
5.11		**Patch-Management**		
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Einspielen von Patches und das Patching erfolgt in einer sinnvollen Kadenz.	1	K
	2	Bei grösseren, bekannten Schwachstellen wird sofort reagiert.	1	K
	3	Der IT-Dienstleister stellt sicher, dass alle relevanten Systeme und Applikationen gepatched werden, neben Betriebssystemen auch Applikationen/Apps, Systeme in der Produktion, Firewall und Netzwerkgeräte. Begründete Ausnahmen sind schriftlich festgehalten.	2	K
	4	Das Patchsystem für Clients ist automatisiert und zentralisiert.	2	K
5.12		**Mobile Devices (Laptops, Tablets, Smartphones)**		
	1	Die Datenträger resp. Container auf mobilen Systemen sind verschlüsselt.	1	I
	2	Der Zugriff auf Firmendaten ist nur nach einer ausreichenden Authentifizierung möglich.	1	I
	3	Es existieren Anforderungen an die mobilen Geräte, welche durch Policies durchgesetzt werden.	2	I
	4	Ein Device- oder Application-Management wird eingesetzt.	2	S
5.13		**Remote Work / Home Office**		
	1	Remote Work Zugriff ist nur nach einer Mehrfaktor-Authentifizierung möglich.	1	I
	2	Eine Remote Work Richtlinie ist mit Mitarbeitenden vereinbart.	2	I
5.14		**Malware-Protection**		
	1	Alle Systeme sind mit einem Malwareschutz versehen, sofern sie dies technisch zulassen.	1	K
	2	Es wird ein zweistufiges Konzept (Firewall und Client) implementiert.	1	K
	3	Systeme ohne Malwareschutz (z.B. Produktionssysteme) sind netzwerkmässig abzuschotten.	2	I
	4	Eine Endpoint Detection and Responce Lösung ist im Einsatz.	2	S
5.15		**Backup / Restore**		
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Backup/Restore der notwendigen Systeme und Services (z.B. Server, Netzwerk-Komponenten, Cloud Services).	1	K
	2	Das Backup wird regelmässig getestet. Es sind regelmässige Restore-Tests von gesamten Systemen und Services inkl. Daten notwendig.	1	K
	3	Eine ausreichende Sicherungskopie besteht aus mehreren Generationen, ist örtlich getrennt und unveränderbar aufzubewahren.	1	K
	4	Der Zugriff auf die Backup-Infrastruktur erfolgt nicht über das reguläre Identity Management.	2	I
5.16		**Change Management / Incident Management**		
	1	Alle relevanten Änderungen an Systemen und Services (Dienstleister und Kunde) erfolgen nach definierten Prozessen und sind nachvollziehbar protokolliert.	1	S
	2	Alle security relevanten Incidents werden nach einem definierten Prozess behandelt und können nachvollzogen werden.	2	S
5.17		**Protokollierung**		
	1	Der IT-Dienstleister stellt sicher, dass alle System-Protokolle gemäss Vereinbarung aufbewahrt werden (SLA empfohlen).	1	S
	2	Jeder Zugriff des IT-Dienstleisters auf Kundensysteme und Hardwarefehler müssen protokolliert werden.	1	S
5.18		**Monitoring / Schwachstellenmanagement**		
	1	Der IT-Dienstleister betreibt ein Monitoring der Systeme und Services und leitet bei Bedarf geeignete Massnahmen ein.	1	S
	2	Die Sicherheitssysteme werden überwacht. Alarme werden behandelt. (z.B. mit einem SOC)	3	S
	3	Ein Schwachstellen-Management wird betrieben.	2	S
5.19		**Entsorgung von Datenträgern / Löschung von Daten**		
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Entsorgen von Datenträgern.	1	S
	2	Es ist ein Prozess für die Datenlöschung vorhanden	2	S
5.20		**Services von Drittanbietern**		
	1	Der IT-Dienstleister kennt die betreuten Produkte von Drittanbietern und kann ein vergleichbares Niveau der Sicherheit wie bei lokalen Services anbieten.	2	S
	2	Der IT-Dienstleister stellt sicher, dass seine Kunden regelmässig über mögliche Verbesserungen der genutzten Drittanbieterdienste informiert und entsprechende Empfehlungen ausgesprochen werden.	3	S
	3	Der IT-Dienstleister unterstützt den Kunden beim sicheren Einsatz von Produkten und Services von Drittanbietern insbesondere bezüglich Datenschutz und Datenabfluss.	3	S
5.21		**Handhabung Künstliche Intelligenz**		
	1	Die Mitarbeiterrichtlinie umfasst auch den Umgang mit KI	1	K
	2	Das Inventar der benutzten Dienste ist aktuell	2	S
	3	Strategie zum Einsatz Die Strategie zum Einsatz und zur Handhabung von künstlicher Intelligenzist festgelegtund Handhabung künstlicher Intelligenz	3	S

Version 3.0 | 01.03.2026

CyberSeal - Prüfliste

Kap.	Pt.	Kontrolle	Prio	Audit- methode: S=Selbst-deklaration I=Interview K=Konsole
5.22		**Ausbildung der Mitarbeiter**		
	1	Eine Benutzer- und Administrationsrichtlinie (z.B. Acceptable Use Policy) ist definiert und wird angewendet und durchgesetzt	1	K
	2	Der IT-Dienstleister organisiert für eigene Mitarbeitende regelmässige Ausbildungen zum Thema Informationssicherheit und stellt deren Wirksamkeit sicher.	1	K
	3	Der IT-Dienstleister bietet seinen Kunden Awareness-Dienste an oder vermittelt ihm einen Drittanbieter.	2	S
5.23		**Notfallkonzept**		
	1	Ein aktuelles Notfallkonzept ist vorhanden und im Notfall verfügbar. Es berücksichtigt u.a. Daten-Verschlüsselungen und -Offenlegung, sowie Erpressung.	1	K
	2	Das Notfallkonzept wird angemessen und regelmässig getestet.	2	S
	3	Das Notfallkonzept regelt auch den Einbezug von externen Stellen (Polizei, BACS, Versicherungen, unterstützende Firmen usw.).	2	S
	4	Der IT-Dienstleiter bietet seinen Kunden Unterstützung an bei der Erstellung eines zeitgemässen Notfallkonzepts.	2	S
5.24		**Ablaufende Termine**		
	1	Die Ablaufdaten von Informatik-Komponenten (Zertifikate, Lizenzen etc.) werden geführt. Es wird rechtzeitig eine Meldung vor Ablauf generiert.	2	S
	2	Der Kunde wird auf veraltete Hard- und Software inklusive den damit verbundenen Risiken aufmerksam gemacht.	2	S
5.25		**Physische Sicherheit**		
	1	Der Zutritt zu den Räumlichkeiten des IT-Dienstleisters ist kontrolliert und sinnvoll eingeschränkt.	1	I
	2	Der Zutritt zum Datacenter des IT-Dienstleisters ist zu autorisieren und zu protokollieren.	1	I
	3	Kritische IT-Geräte des Dienstleisters sind gegen äussere Einflüsse geschützt (z.B. USV, Kühlung, redundanter Internet Anschluss).	2	I
5.26		**IT-Risikomanagement**		
	1	Es wird jährlich ein Risikomanagement / Risikoanalyse durchgeführt. Der VR unterzeichnet den Risk Report zu Handen der GL und akzeptiert damit die verbleibenden Risiken.	2	I
	2	Es wurde ein Prozess etabliert, um nicht akzeptable Risiken zu behandeln.	2	I
	3	Der IT-Dienstleister unterstützt den Kunden bei Bedarf in den Fragen des Risiko-Managements.	3	S
	4	Im IT-Risikomanagement muss Digital Resillience berücksichtigt sein.	3	S
5.27		**Datenschutz und Rechtliches**		
	1	Relevante gesetzliche und regulatorische Anforderungen (z. B. DSG, ISG) sind bekannt und werden berücksichtigt.	1	S
	2	Betroffenheitsabklärung wurde durchgeführt und Meldepflichtprozess ist vorhanden	2	S
	3	IT-Dienstleister begleitet Kunden bei Bedarf mit Anforderungen DSG, ISG (Betroffenheitsabklärung, Meldepflicht)	2	S
5.28		**Softwareentwicklung**		
	1	Die grundlegenden Prinzipien der sicheren Softwareentwicklung (z. B. OWASP Top 10) werden konsequent angewendet. Die Softwareentwicklung erfolgt nach einem definierten Prozess.	1	I
	2	Sicherheitsaspekte sind im Code-Review-Prozess integriert.	3	S
	3	Ein Prozess stellt sicher, dass bei der Entwicklung Protokolldateien und Fehlermeldungen keine sensiblen Informationen preisgeben und sicher verarbeitet werden.	2	I
	4	Bei der Entwicklung werden systematisch Sicherheits-Tools und -Tests (z. B. statische/dynamische Analyse, Penetrationstests) zur Ermittlung von Schwachstellen eingesetzt.	3	S