ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Management Service

ZERTIFIKAT

Zertifikat-Registrier-Nr.: **12 310 40834 TMS** / Auftrags-Nr.: **70775393**

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH

bescheinigt, dass die Organisation

plusserver

plusserver gmbh
Venloer Str. 47
50672 Köln
Deutschland

für den Geltungsbereich

Bereitstellung und Betrieb der Cloud-Services 'pluscloud VMware', 'pluscloud open' und 'plusserver Kubernetes Engine' sowie der für die Cloud und Hosting Services genutzten Rechenzentrumskapazitäten und Netzwerkanbindungen in den Standorten Köln (CGN3), Düsseldorf (DUS6), Hamburg/Norderstedt (HAM5) und Hamburg Wilhelmsburg (HAM6)

einschließlich der Standorte gemäß Anlage

ein Informationssicherheitsmanagementsystem gemäß
„Erklärung zur Anwendbarkeit“ eingeführt hat und anwendet.

Durch ein Audit wurde der Nachweis erbracht,
dass die Forderungen der

ISO/IEC 27001:2022

erfüllt sind.

Dieses Zertifikat ist gültig vom **04.10.2024** bis **31.05.2026**.

Version der Erklärung zur Anwendbarkeit: **V4.0 vom 26.06.2024**

Fred Wenke
Leiter der Zertifizierungsstelle
München, 08.10.2024

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuvsud.com/de-certificate-validity-check

TÜV®

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Management Service

ANLAGE ZUM ZERTIFIKAT

Zertifikat-Registrier-Nr.: **12 310 40834 TMS** / Auftrags-Nr.: **70775393**

Zertifikatshalter:

plusserver gmbh
Venloer Str. 47
50672 Köln
Deutschland

an den Standorten	Geltungsbereich
plusserver gmbh Venloer Str. 47 50672 Köln Deutschland	Bereitstellung und Betrieb der Cloud-Services 'pluscloud VMware', 'pluscloud open' und 'plusserver Kubernetes Engine'
plusserver gmbh Welserstraße 14 51149 Köln Deutschland	Bereitstellung und Betrieb der für die Cloud und Hosting Services genutzten Rechenzentrumskapazitäten und Netzwerkanbindungen in den Standorten Köln (CGN3), Düsseldorf (DUS6), Hamburg/Norderstedt (HAM5) und Hamburg Wilhelmsburg (HAM6)
plusserver gmbh In der Steele 33a-41 40599 Düsseldorf Deutschland	Bereitstellung und Betrieb der für die Cloud und Hosting Services genutzten Rechenzentrumskapazitäten und Netzwerkanbindungen (DUS6)
plusserver gmbh Altmarkt 25 01067 Dresden Deutschland	Betrieb der Cloud und Hosting Services
plusserver gmbh Neustädter Neuer Weg 22 20459 Hamburg Deutschland	Bereitstellung und Betrieb der für die Cloud und Hosting Services genutzten Rechenzentrumskapazitäten und Netzwerkanbindungen in den Standorten Hamburg/Norderstedt (HAM5) und Hamburg Wilhelmsburg (HAM6)

Fred Wenke
Leiter der Zertifizierungsstelle
München, 08.10.2024

DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuvsud.com/de-certificate-validity-check

TÜV®

ISO 27001:2022 - Statement of Applicabilty

Nr.	Kontrollen ISO 27001:2022	Beschreibung der Kontrollen	Anwendbar	Status	Begründung der (Nicht-)Anwendbarkeit
A.5 Organisatorische Kontrollen					
A.5.1	Richtlinien für die Informationssicherheit	Informationssicherheitsrichtlinien und themenspezifische Richtlinien müssen definiert, vom Management genehmigt, veröffentlicht, den relevanten Mitarbeitern und relevanten interessierten Parteien mitgeteilt und von diesen anerkannt werden.	ja	100%	Geschäftliche Anforderung
A.5.2	Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit	Rollen und Verantwortlichkeiten für die Informationssicherheit müssen entsprechend den Anforderungen der Organisation definiert und zugewiesen werden.	ja	100%	Geschäftliche Anforderung
A.5.3	Aufgabentrennung	Miteinander in Konflikt stehende Aufgaben und Zuständigkeitsbereiche müssen getrennt werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.4	Verantwortlichkeiten des Managements	Das Management muss von allen Mitarbeitern verlangen, dass sie Informationssicherheit in Übereinstimmung mit der festgelegten Informationssicherheitsrichtlinie sowie den themenspezifischen Richtlinien und Verfahren der Organisation anwenden.	ja	100%	Geschäftliche Anforderung
A.5.5	Kontakt mit Behörden	Die Organisation muss Kontakte zu den zuständigen Behörden herstellen und aufrechterhalten.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.6	Kontakt mit besonderen Interessengruppen	Die Organisation muss Kontakte zu speziellen Interessengruppen oder anderen spezialisierten Sicherheitsforen und Berufsverbänden herstellen und pflegen.	ja	100%	Geschäftliche Anforderung
A.5.7	Bedrohungsanalyse	Informationen zu Bedrohungen der Informationssicherheit werden gesammelt und analysiert, um Bedrohungsinformationen zu erstellen.	ja	100%	Geschäftliche Anforderung
A.5.8	Informationssicherheit im Projektmanagement	Informationssicherheit soll in das Projektmanagement integriert werden.	ja	100%	Geschäftliche Anforderung
A.5.9	Inventarisierung von Informationen und anderen zugehörigen Vermögenswerten	Es ist ein Inventar der Informationen und anderer damit verbundener Vermögenswerte, einschließlich der Eigentümer, zu erstellen und zu pflegen.	ja	100%	Geschäftliche Anforderung
A.5.10	Akzeptable Nutzung von Informationen und anderen zugehörigen Vermögenswerten	Regeln für die akzeptable Nutzung und Verfahren für den Umgang mit Informationen und anderen damit verbundenen Vermögenswerten müssen identifiziert, dokumentiert und umgesetzt werden.	ja	100%	Geschäftliche Anforderung
A.5.11	Rückgabe von Vermögenswerten	Das Personal und gegebenenfalls andere interessierte Parteien müssen bei Änderung oder Beendigung ihres Arbeitsverhältnisses, Vertrags oder ihrer Vereinbarung alle in ihrem Besitz befindlichen Vermögenswerte der Organisation zurückgeben.	ja	100%	Geschäftliche Anforderung
A.5.12	Klassifizierung von Informationen	Informationen werden entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen interessierter Parteien klassifiziert.	ja	100%	Geschäftliche Anforderung
A.5.13	Kennzeichnung von Informationen	Entsprechend dem von der Organisation angenommenen Informationsklassifizierungsschema müssen geeignete Verfahren zur Informationskennzeichnung entwickelt und umgesetzt werden.	ja	100%	Geschäftliche Anforderung
A.5.14	Informationsübertragung	Für alle Arten von Übermittlungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung bestehen.	ja	100%	Geschäftliche Anforderung
A.5.15	Zugangskontrolle	Regeln zur Kontrolle des physischen und logischen Zugangs zu Informationen und anderen zugehörigen Vermögenswerten werden auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt.	ja	100%	Geschäftliche Anforderung
A.5.16	Identitätsmanagement	Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.	ja	100%	Geschäftliche Anforderung
A.5.17	Authentifizierungsinformationen	Die Zuteilung und Verwaltung von Authentifizierungsinformationen wird durch einen Managementprozess gesteuert, der auch die Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen umfasst.	ja	100%	Geschäftliche Anforderung

ISO 27001:2022 - Statement of Applicabilty

Nr.	Kontrollen ISO 27001:2022	Beschreibung der Kontrollen	Anwendbar	Status	Begründung der (Nicht-)Anwendbarkeit
A.5 Organisatorische Kontrollen					
A.5.18	Zugriffsrechte	Zugriffsrechte auf Informationen und andere zugehörige Ressourcen werden in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugriffskontrolle vergeben, überprüft, geändert und entfernt.	ja	100%	Geschäftliche Anforderung
A.5.19	Informationssicherheit in Lieferantenbeziehungen	Es sind Prozesse und Verfahren festzulegen und umzusetzen, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.20	Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen	Die einschlägigen Anforderungen an die Informationssicherheit werden je nach Art der Lieferbeziehung mit jedem Lieferanten festgelegt und vereinbart.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.21	Management der Informationssicherheit in der Lieferkette der Informations- und Kommunikations-technologie (IKT)	Es sind Prozesse und Verfahren festzulegen und umzusetzen, um die mit der Lieferkette für IKT-Produkte und -Dienstleistungen verbundenen Informationssicherheitsrisiken zu beherrschen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferdiensten	Die Organisation muss regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.23	Informationssicherheit bei der Nutzung von Cloud-Diensten	Prozesse für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten müssen in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation eingerichtet werden.	ja	100%	Geschäftliche Anforderung
A.5.24	Planung und Vorbereitung des Managements von Informationssicherheitsvorfällen	Die Organisation muss das Management von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für das Management von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.	ja	100%	Geschäftliche Anforderung
A.5.25	Bewertung und Entscheidung über Ereignisse im Bereich der Informationssicherheit	Die Organisation muss Ereignisse im Bereich der Informationssicherheit bewerten und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden sollen.	ja	100%	Geschäftliche Anforderung
A.5.26	Reaktion auf Informationssicherheitsvorfälle	Auf Vorfälle im Bereich der Informationssicherheit ist gemäß den dokumentierten Verfahren zu reagieren.	ja	100%	Geschäftliche Anforderung
A.5.27	Lehren aus Informationssicherheitsvorfällen	Die aus Vorfällen im Bereich der Informationssicherheit gewonnenen Erkenntnisse werden zur Stärkung und Verbesserung der Informationssicherheitskontrollen genutzt.	ja	100%	Geschäftliche Anforderung
A.5.28	Sammeln von Beweismaterial	Die Organisation muss Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismitteln im Zusammenhang mit Informationssicherheitsvorfällen einführen und umsetzen.	ja	100%	Geschäftliche Anforderung
A.5.29	Informationssicherheit während Störungen	Die Organisation muss planen, wie die Informationssicherheit während einer Unterbrechung auf einem angemessenen Niveau gehalten werden kann.	ja	100%	Geschäftliche Anforderung
A.5.30	IKT-Bereitschaft für Geschäftskontinuität	Die IKT-Bereitschaft muss auf der Grundlage von Geschäftskontinuitätszielen und IKT-Kontinuitätsanforderungen geplant, implementiert, aufrechterhalten und getestet werden.	ja	100%	Geschäftliche Anforderung
A.5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit von Bedeutung sind, sowie der Ansatz der Organisation zur Erfüllung dieser Anforderungen müssen ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.32	Geistige Eigentumsrechte	Die Organisation muss geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum anwenden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.33	Schutz von Aufzeichnungen	Aufzeichnungen sind vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Freigabe zu schützen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.5.34	Privatsphäre und Schutz von personenbezogenen Daten (pbD)	Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten gemäß den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe

ISO 27001:2022 - Statement of Applicabilty

Nr.	Kontrollen ISO 27001:2022	Beschreibung der Kontrollen	Anwendbar	Status	Begründung der (Nicht-)Anwendbarkeit
A.5 Organisatorische Kontrollen					
A.5.35	Unabhängige Überprüfung der Informationssicherheit	Der Ansatz der Organisation für das Management der Informationssicherheit und seine Umsetzung, einschließlich der Mitarbeiter, Verfahren und Technologien, ist in geplanten Abständen oder bei wesentlichen Änderungen unabhängig zu überprüfen.	ja	100%	Geschäftliche Anforderung
A.5.36	Einhaltung von Strategien, Regeln und Standards für die Informationssicherheit	Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Standards ist regelmäßig zu überprüfen.	ja	100%	Geschäftliche Anforderung
A.5.37	Dokumentierte Betriebsverfahren	Die Betriebsverfahren für Informationsverarbeitungsanlagen sind zu dokumentieren und dem Personal, das sie benötigt, zur Verfügung zu stellen.	ja	100%	Geschäftliche Anforderung
A.6 Personal-Kontrollen					
A.6.1	Personal-Überprüfung	Die Überprüfung des Hintergrunds aller Kandidaten, die in das Personal aufgenommen werden sollen, muss vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung der geltenden Gesetze, Vorschriften und ethischen Grundsätze durchgeführt werden und müssen in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Klassifizierung der Informationen, auf die zugegriffen werden soll, und den wahrgenommenen Risiken stehen.	ja	100%	Geschäftliche Anforderung
A.6.2	Arbeits- und Beschäftigungsbedingungen	In den arbeitsvertraglichen Vereinbarungen müssen die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.6.3	Sensibilisierung für die Informationssicherheit, Aufklärung und Schulung	Das Personal der Organisation und relevante interessierte Parteien erhalten eine angemessene Sensibilisierung für die Informationssicherheit, Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren, die für ihre jeweilige Funktion relevant sind.	ja	100%	Geschäftliche Anforderung
A.6.4	Disziplinarverfahren	Es ist ein Disziplinarverfahren zu formalisieren und zu kommunizieren, um Maßnahmen gegen Mitarbeiter und andere Beteiligte zu ergreifen, die gegen die Informationssicherheitspolitik verstoßen haben.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.6.5	Verantwortlichkeiten nach Beendigung oder Wechsel des Beschäftigungsverhältnisses	Die Zuständigkeiten und Pflichten im Bereich der Informationssicherheit, die nach Beendigung oder Wechsel des Beschäftigungsverhältnisses fortbestehen, sind festzulegen, durchzusetzen und den betreffenden Mitarbeitern und anderen interessierten Parteien mitzuteilen.	ja	100%	Geschäftliche Anforderung
A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die den Informationsschutzbedarf der Organisation widerspiegeln, sind zu ermitteln, zu dokumentieren, regelmäßig zu überprüfen und von den Mitarbeitern und anderen betroffenen Parteien zu unterzeichnen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.6.7	Remote-Arbeiten	Für Mitarbeiter, die aus der Ferne arbeiten, sind Sicherheitsmaßnahmen zu ergreifen, um Informationen zu schützen, die außerhalb der Räumlichkeiten der Organisation abgerufen, verarbeitet oder gespeichert werden.	ja	100%	Geschäftliche Anforderung
A.6.8	Berichterstattung über Ereignisse im Bereich der Informationssicherheit	Die Organisation muss einen Mechanismus bereitstellen, der es dem Personal ermöglicht, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit über geeignete Kanäle rechtzeitig zu melden.	ja	100%	Geschäftliche Anforderung
A.7 Physische Kontrollen					
A.7.1	Physische Sicherheitsperimeter	Zum Schutz von Bereichen, die Informationen und andere zugehörige Werte enthalten, sind Sicherheitsabgrenzungen festzulegen und zu verwenden.	ja	100%	Geschäftliche Anforderung
A.7.2	Physischer Zugang	Die Sicherheitsbereiche sind durch geeignete Zugangskontrollen und Zugangspunkte zu schützen.	ja	100%	Geschäftliche Anforderung
A.7.3	Sicherung von Büros, Räumen und Anlagen	Die physische Sicherheit von Büros, Räumen und Anlagen ist zu konzipieren und umzusetzen.	ja	100%	Geschäftliche Anforderung
A.7.4	Überwachung der physischen Sicherheit	Die Räumlichkeiten müssen kontinuierlich auf unbefugten physischen Zutritt überwacht werden.	ja	100%	Geschäftliche Anforderung
A.7 Physische Kontrollen					

ISO 27001:2022 - Statement of Applicabilty

Nr.	Kontrollen ISO 27001:2022	Beschreibung der Kontrollen	Anwendbar	Status	Begründung der (Nicht-)Anwendbarkeit
A.7.5	Schutz vor physischen und Umweltbedrohungen	Der Schutz vor physischen und umweltbedingten Bedrohungen, wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur, ist zu konzipieren und umzusetzen.	ja	100%	Geschäftliche Anforderung
A.7.6	Arbeiten in Sicherheitsbereichen	Es sind Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen zu konzipieren und umzusetzen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.7.7	Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms	Es werden klare Regeln für den Umgang mit Papieren und Wechseldatenträgern auf dem Schreibtisch und klare Regeln für den Umgang mit Bildschirmen in Informationsverarbeitungsanlagen festgelegt und in geeigneter Weise durchgesetzt.	ja	100%	Geschäftliche Anforderung
A.7.8	Standortwahl und Schutz von Geräten	Geräte müssen sicher und geschützt aufgestellt werden.	ja	100%	Geschäftliche Anforderung
A.7.9	Sicherheit von Vermögenswerten außerhalb von Geschäftsräumen	Vermögenswerte außerhalb des Standorts müssen geschützt werden.	ja	100%	Geschäftliche Anforderung
A.7.10	Speichermedien	Speichermedien müssen während ihres gesamten Lebenszyklus - Erwerb, Verwendung, Transport und Entsorgung - gemäß dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.	ja	100%	Geschäftliche Anforderung
A.7.11	Unterstützende Versorgungseinrichtungen	Die Informationsverarbeitungseinrichtungen sind vor Stromausfällen und anderen durch Ausfälle der Versorgungseinrichtungen verursachten Störungen zu schützen.	ja	100%	Geschäftliche Anforderung
A.7.12	Sicherheit der Verkabelung	Kabel, die Energie, Daten oder unterstützende Informationsdienste transportieren, müssen vor Abhören, Störungen oder Schäden geschützt werden.	ja	100%	Geschäftliche Anforderung
A.7.13	Instandhaltung der Geräte	Die Geräte müssen ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen zu gewährleisten.	ja	100%	Geschäftliche Anforderung
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten	Geräte, die Speichermedien enthalten, müssen überprüft werden, um sicherzustellen, dass alle sensiblen Daten und lizenzierte Software vor der Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben wurden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.8 Technologische Kontrollen					
A.8.1	Benutzerendgeräte	Informationen, die auf Endgeräten des Nutzers gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, müssen geschützt werden.	ja	100%	Geschäftliche Anforderung
A.8.2	Privilegierte Zugriffsrechte	Die Zuweisung und Nutzung privilegierter Zugriffsrechte ist zu beschränken und zu verwalten.	ja	100%	Geschäftliche Anforderung
A.8.3	Beschränkung des Zugangs zu Informationen	Der Zugang zu Informationen und anderen zugehörigen Vermögenswerten wird gemäß der festgelegten themenspezifischen Richtlinien zur Zugangskontrolle eingeschränkt.	ja	100%	Geschäftliche Anforderung
A.8.4	Zugang zu Quellcode	Der Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken muss angemessen verwaltet werden.	ja	100%	Geschäftliche Anforderung
A.8.5	Sichere Authentifizierung	Sichere Authentifizierungstechnologien und -verfahren sind auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Sicherheitsrichtlinie zur Zugangskontrolle zu implementieren.	ja	100%	Geschäftliche Anforderung
A.8.6	Kapazitätsmanagement	Die Nutzung der Ressourcen wird überwacht und entsprechend dem aktuellen und erwarteten Kapazitätsbedarf angepasst.	ja	100%	Geschäftliche Anforderung
A.8.7	Schutz vor Schadprogrammen	Der Schutz vor Schadsoftware muss durch eine angemessene Sensibilisierung der Benutzer unterstützt werden.	ja	100%	Geschäftliche Anforderung
A.8.8	Management technischer Schwachstellen	Es sind Informationen über technische Schwachstellen der verwendeten Informationssysteme einzuholen, die Gefährdung der Organisation durch solche Schwachstellen zu bewerten und geeignete Maßnahmen zu ergreifen.	ja	100%	Geschäftliche Anforderung
A.8.9	Konfigurationsmanagement	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen eingerichtet, dokumentiert, implementiert, überwacht und überprüft werden.	ja	100%	Geschäftliche Anforderung
A.8 Technologische Kontrollen					

ISO 27001:2022 - Statement of Applicabilty

Nr.	Kontrollen ISO 27001:2022	Beschreibung der Kontrollen	Anwendbar	Status	Begründung der (Nicht-)Anwendbarkeit
A.8.10	Löschung von Informationen	In Informationssystemen, Geräten oder anderen Speichermedien gespeicherte Informationen werden gelöscht, wenn sie nicht mehr benötigt werden.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.8.11	Datenmaskierung	Die Datenmaskierung muss in Übereinstimmung mit der themenspezifischen Richtlinie der Organisation zur Zugriffskontrolle und anderen verwandten themenspezifischen Richtlinien sowie den Geschäftsanforderungen unter Berücksichtigung der geltenden Gesetzgebung verwendet werden.	ja	100%	Geschäftliche Anforderung
A.8.12	Verhinderung von Datenverlusten	Maßnahmen zur Verhinderung von Datenlecks müssen auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.8.13	Datensicherung	Sicherungskopien von Informationen, Software und Systemen werden gemäß den vereinbarten themenspezifischen Grundsätzen für die Datensicherung aufbewahrt und regelmäßig getestet.	ja	100%	Geschäftliche Anforderung
A.8.14	Redundanz der Informationsverarbeitungs-anlagen	Die Einrichtungen zur Informationsverarbeitung müssen so redundant ausgelegt sein, dass sie die Anforderungen an die Verfügbarkeit erfüllen.	ja	100%	Geschäftliche Anforderung
A.8.15	Protokollierung	Es sind Protokolle zu erstellen, zu speichern, zu schützen und zu analysieren, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen.	ja	100%	Geschäftliche Anforderung
A.8.16	Überwachung von Aktivitäten	Netzwerke, Systeme und Anwendungen müssen auf anomales Verhalten überwacht und geeignete Maßnahmen ergriffen werden, um potenzielle Vorfälle im Bereich der Informationssicherheit zu bewerten.	ja	100%	Geschäftliche Anforderung
A.8.17	Synchronisierung der Uhrzeit	Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme müssen mit zugelassenen Zeitquellen synchronisiert werden.	ja	100%	Geschäftliche Anforderung
A.8.18	Verwendung von privilegierten Dienstprogrammen	Die Verwendung von Hilfsprogrammen, die in der Lage sind, die System- und Anwendungssteuerung außer Kraft zu setzen, muss eingeschränkt und streng kontrolliert werden.	ja	100%	Geschäftliche Anforderung
A.8.19	Installation von Software auf operativen Systemen	Es sind Verfahren und Maßnahmen zu ergreifen, um die Installation von Software auf den Betriebssystemen sicher zu verwalten.	ja	100%	Geschäftliche Anforderung
A.8.20	Netzwerksicherheit	Netze und Netzgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.	ja	100%	Geschäftliche Anforderung
A.8.21	Sicherheit von Netzwerkdiensten	Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzdienste sind zu ermitteln, umzusetzen und zu überwachen.	ja	100%	Geschäftliche Anforderung
A.8.22	Trennung von Netzwerken	Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in den Netzen der Organisation getrennt werden.	ja	100%	Geschäftliche Anforderung
A.8.23	Web-Filterung	Der Zugriff auf externe Websites muss verwaltet werden, um die Gefährdung durch schädliche Inhalte zu verringern.	ja	100%	Geschäftliche Anforderung
A.8.24	Einsatz von Kryptografie	Es werden Regeln für den wirksamen Einsatz der Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt.	ja	100%	Geschäftliche Anforderung
A.8.25	Sicherer Entwicklungslebenszyklus	Es sind Regeln für die sichere Entwicklung von Software und Systemen aufzustellen und anzuwenden.	ja	100%	Geschäftliche Anforderung
A.8.26	Anforderungen an die Anwendungssicherheit	Die Anforderungen an die Informationssicherheit müssen bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.	ja	100%	Geschäftliche Anforderung
A.8.27	Sichere Systemarchitektur und technische Grundsätze	Es sind Grundsätze für die Entwicklung sicherer Systeme festzulegen, zu dokumentieren, aufrechtzuerhalten und bei allen Tätigkeiten zur Entwicklung von Informationssystemen anzuwenden.	ja	100%	Geschäftliche Anforderung
A.8.28	Sichere Programmierung	Bei der Softwareentwicklung sind die Grundsätze der sicheren Kodierung anzuwenden.	ja	100%	Geschäftliche Anforderung
A.8.29	Sicherheitstests in Entwicklung und Abnahme	Die Verfahren für die Sicherheitsprüfung sind zu definieren und in den Lebenszyklus der Entwicklung einzubeziehen.	ja	100%	Geschäftliche Anforderung
A.8.30	Ausgelagerte Entwicklung	Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgelagerten Systementwicklung leiten, überwachen und überprüfen.	ja	100%	Geschäftliche Anforderung
A.8 Technologische Kontrollen					

ISO 27001:2022 - Statement of Applicabilty

Nr.	Kontrollen ISO 27001:2022	Beschreibung der Kontrollen	Anwendbar	Status	Begründung der (Nicht-)Anwendbarkeit
A.8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	Entwicklungs-, Test- und Produktionsumgebungen müssen getrennt und gesichert sein.	ja	100%	Geschäftliche Anforderung
A.8.32	Änderungsmanagement	Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen unterliegen den Verfahren des Änderungsmanagements.	ja	100%	Geschäftliche Anforderung
A.8.33	Test-Informationen	Die Testinformationen sind in geeigneter Weise auszuwählen, zu schützen und zu verwalten.	ja	100%	Geschäftliche Anforderung Gesetzliche Vorgabe
A.8.34	Schutz der Informationssysteme während der Prüfung	Audittests und andere Versicherungstätigkeiten, die eine Bewertung der operativen Systeme beinhalten, werden zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart.	ja	100%	Geschäftliche Anforderung