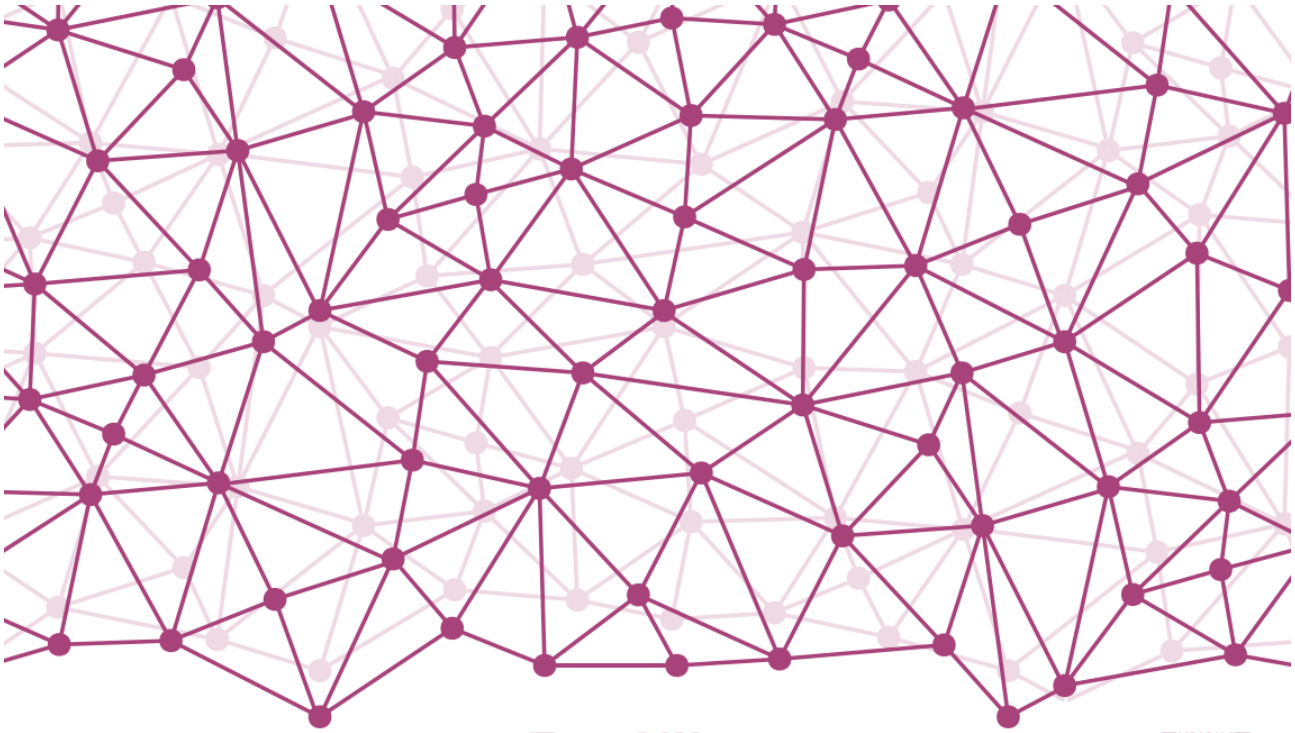
Erklärung zur Anwendbarkeit (SOA)

nach ISO/IEC 27001:2022

vom 06.03.24

Vertraulich

Vertragspartner	
Ansprechpartner	
Leistender	Silpion IT-Services GmbH Brandshofer Deich 48 20539 Hamburg
Ansprechpartner	*Jaroslaw Zdrzalek*



Zertifikat

Silpion IT-Services GmbH, Brandshofer Deich 48, 20539 Hamburg, Deutschland

Die **CERTIVATION** GmbH bescheinigt der oben benannten Organisation hiermit, dass das Informationssicherheitsmanagementsystem (ISMS) für den unten genannten Geltungsbereich (Scope) auf Grundlage des Statements of Applicability, Version 1 die Anforderungen der folgenden internationalen Norm erfüllt:

ISO/IEC 27001:2022

Geltungsbereich:

Engineering, Operations und Support von Cloud und hybriden Infrastrukturen.

Lingen, 04.03.2024

Ort, Datum

ISO/IEC 27001

Unterschrift
Leiter der Zertifizierungsstelle

Gültig von: 04.03.2024
Gültig bis: 03.03.2027
Zertifikats-ID: 27001-27600147

CERTivation

CERTIVATION GmbH, Am Seitenkanal 8, 49811 Lingen (Ems), Deutschland

Blockchain: https://explorer.certivation.com/explorer/contracts?address=0x9B1892D9CF9951e7ae23a1fA93Cc8C6c38229C924

Version 1.0

1 Angaben zu diesem Dokument

1.1 Rechtevorbehalt

1.2 Versionsangaben

Version	Datum	Autor	Kommentar
1		JZ	Initialversion
1.3	06.03.24	JZ	Arbeitsversion

1.3 Generisches Maskulinum

In diesem Dokument wird aus Gründen der Lesbarkeit durchgängig die männliche Form verwendet. Sie soll geschlechtsneutral interpretiert werden.

2 Erklärung zur Anwendbarkeit (SoA)

Anhang A 27001:2022			
Kapitel	**Maßnahme**	**Anforderung**	**umgesetzt**
5.1	Informationssicherheitsleitlinien	Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.	**X**
5.2	Informationssicherheitsrollen und- verantwortlichkeiten	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.	**X**
5.3	Aufgabentrennung	Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.	**X**
5.4	Verantwortlichkeiten der Leitung	Die Leitung muss von dem gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.	**X**
5.5	Kontakt mit Behörden	Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.	**X**
5.6	Kontakt mit speziellen Interessensgruppen	Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.	**X**
5.7	Erkenntnisse über Bedrohungen	Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.	**X**
5.8	Informationssicherheit im Projektmanagement	Die Informationssicherheit muss in das Projektmanagement integriert werden.	**X**
5.9	Inventar der Informationen und anderen damit verbundenen Werten	Ein Inventar der Informationen und anderen damit verbundenen Werten, einschließlich der Eigentümer, muss erstellt und gepflegt werden.	**X**
5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten müssen aufgestellt, dokumentiert und angewendet werden.	**X**
5.11	Rückgabe von Werten	Das Personal und gegebenenfalls andere interessierte Parteien müssen alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.	**X**
5.12	Klassifizierung von Information	Informationen müssen entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.	**X**
5.13	Kennzeichnung von Information	Ein angemessener Satz von Verfahren zur Kennzeichnung von Information muss entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.	**X**
5.14	Informationsübertragung	Für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.	**X**
5.15	Zugangssteuerung	Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere zugehörige Werte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.	**X**
5.16	Identitätsmanagement	Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.	**X**
5.17	Informationen zur Authentifizierung	Die Zuweisung und Verwaltung von Authentifizierungsinformationen muss durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen umfasst.	**X**
5.18	Zugangsrechte	Zugangsrechte zu Informationen und anderen zugehörigen Werten müssen in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.	**X**

5.19	Informationssicherheit in Lieferantenbeziehungen	Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.	**X**
5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Je nach Art der Lieferantenbeziehung müssen die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.	**X**
5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)	Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.	**X**
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	Die Organisation muss regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.	**X**
5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten müssen in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.	**X**
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	Die Organisation muss die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.	**X**
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	Die Organisation muss Ereignisse im Bereich der Informationssicherheit beurteilen und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden müssen.	**X**
5.26	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.	**X**
5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse müssen zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.	**X**
5.28	Sammeln von Beweismaterial	Die Organisation muss Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismaterial im Zusammenhang mit Informationssicherheitsvorfällen einführen und umsetzen.	**X**
5.29	Informationssicherheit bei Störungen	Die Organisation muss planen, wie die Informationssicherheit während einer Störung auf einem angemessenen Niveau gehalten werden kann.	**X**
5.30	IKT-Bereitschaft für Business Continuity	Die IKT-Bereitschaft muss auf der Grundlage von Business-Continuity- Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.	**X**
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungen müssen ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.	**X**
5.32	Geistige Eigentumsrechte	Die Organisation muss geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.	**X**
5.33	Schutz von Aufzeichnungen	Aufzeichnungen müssen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.	**X**
5.34	Privatsphäre und Schutz von personenbezogenen Daten(PbD)	Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.	**X**
5.35	Unabhängige Überprüfung der Informationssicherheit	Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung einschließlich der Mitarbeiter, Prozesse und Technologien, müssen auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.	**X**
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Normen muss regelmäßig überprüft werden.	**X**
5.37	Dokumentierte Bedienabläufe	Die Betriebsverfahren für Informationsverarbeitungsanlagen müssen dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.	**X**

6.1	Sicherheitsüberprüfung	Alle Personen, die in die Belegschaft aufgenommen werden, müssen vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung geltender Gesetze, Vorschriften und ethischer Grundsätze einer Sicherheitsüberprüfung unterzogen werden und diese Überprüfung muss in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken stehen.	**X**
6.2	Beschäftigungs- und Vertragsbedingungen	In den arbeitsvertraglichen Vereinbarungen müssen die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.	**X**
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Das Personal der Organisation und relevante interessierte Parteien müssen ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet relevant sind.	**X**
6.4	Maßregelungsprozess	Ein Maßregelungsprozess muss formalisiert und kommuniziert werden, um Maßnahmen gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitspolitik begangen haben.	**X**
6.5	Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, müssen festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.	**X**
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, müssen identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.	**X**
6.7	Telearbeit	Es müssen Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter extern arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.	**X**
6.8	Meldung von Informationssicherheitsereignissen	Die Organisation muss einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit über geeignete Kanäle rechtzeitig zu melden.	**X**
7.1	Physische Sicherheitsperimeter	Zum Schutz von Bereichen, in denen sich andere zugehörige Werte befinden, müssen Sicherheitsperimeter festgelegt und verwendet werden.	**X**
7.2	Physischer Zutritt	Sicherheitsbereiche müssen durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.	**X**
.3	Sichern von Büros, Räumen und Einrichtungen	Die physische Sicherheit für Büros, Räume und Einrichtungen muss konzipiert und umgesetzt werden.	**X**
7.4	Physische Sicherheitsüberwachung	Die Räumlichkeiten müssen ständig auf unbefugten physischen Zugang überwacht werden.	**X**
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur muss konzipiert und umgesetzt werden.	**X**
7.6	Arbeiten in Sicherheitsbereichen	Es müssen Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.	**X**
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Es müssen klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.	**X**
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen sicher und geschützt aufgestellt werden.	**X**
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	Werte außerhalb des Standorts müssen geschützt werden.	**X**
7.10	Speichermedien	Speichermedien müssen während ihres gesamten Lebenszyklus– Erwerb, Verwendung, Transport und Entsorgung - in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.	**X**
7.11	Versorgungseinrichtungen	Informationsverarbeitungseinrichtungen müssen vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.	**X**
7.12	Sicherheit der Verkabelung	Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, müssen vor Unterbrechung, Störung oder Beschädigung geschützt werden.	**X**

7.13	Instandhalten von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.	**X**
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, müssen überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.	**X**
8.1	Endpunktgeräte des Benutzers	Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, müssen geschützt werden.	**X**
8.2	Privilegierte Zugangsrechte	Zuteilung und Gebrauch von privilegierten Zugangsrechten müssen eingeschränkt und verwaltet werden.	**X**
8.3	Informationszugangsbeschränkung	Der Zugang zu Informationen und anderen zugehörigen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.	**X**
8.4	Zugriff auf den Quellcode	Der Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken müssen angemessen verwaltet werden.	**X**
8.5	Sichere Authentifizierung	Sichere Authentifizierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert werden.	**X**
8.6	Kapazitätssteuerung	Die Nutzung von Ressourcen muss überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.	**X**
8.7	Schutz gegen Schadsoftware	Schutz gegen Schadsoftware muss umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.	**X**
8.8	Handhabung von technischen Schwachstellen	Es müssen Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.	**X**
8.9	Konfigurationsmanagement	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.	**X**
8.10	Löschung von Informationen	Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, müssen gelöscht werden, wenn sie nicht mehr benötigt werden.	**X**
8.11	Datenmaskierung	Die Datenmaskierung muss in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden.	**X**
8.12	Verhinderung von Datenlecks	Maßnahmen zur Verhinderung von Datenlecks müssen auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.	**X**
8.13	Sicherung von Information	Sicherungskopien von Informationen, Software und Systemen müssen in Übereinstimmung mit den vereinbarten themenspezifischen Richtlinien für Datensicherungen aufbewahrt und regelmäßig geprüft werden.	**X**
8.14	Redundanz von informationsverarbeitenden Einrichtungen	Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert werden.	**X**
8.15	Protokollierung	Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.	**X**
8.16	Überwachung von Aktivitäten	Netzwerke, Systeme und Anwendungen müssen auf unübliches Verhalten überwacht und geeignete Maßnahmen müssen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.	**X**
8.17	Uhrensynchronisation	Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme müssen mit zugelassenen Zeitquellen synchronisiert werden.	**X**
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Der Gebrauch von Hilfsprogrammen, die fähig sein können, System- und Anwendungsschutzmaßnahmen zu umgehen, muss eingeschränkt und streng überwacht werden.	**X**
8.19	Installation von Software auf Systemen im Betrieb	Es müssen Verfahren und Maßnahmen umgesetzt werden, um die Installation von Software auf Betriebssystemen sicher zu verwalten.	**X**

8.20	Netzwerksicherheit	Netzwerke und Netzwerkgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.	**X**
8.21	Sicherheit von Netzwerkdiensten	Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste müssen ermittelt, umgesetzt und überwacht werden.	**X**
8.22	Trennung von Netzwerken	Informationsdienste, Benutzer und Informationssysteme müssen in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.	**X**
8.23	Webfilterung	Der Zugang zu externen Websites muss verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.	**X**
8.24	Verwendung von Kryptographie	Es müssen Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.	**X**
8.25	Lebenszyklus einer sicheren Entwicklung	Regeln für die sichere Entwicklung von Software und Systemen müssen festgelegt und angewendet werden.	**X**
8.26	Anforderungen an die Anwendungssicherheit	Die Anforderungen an die Informationssicherheit müssen bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.	**X**
8.27	Sichere Systemarchitektur und technische Grundsätze	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme müssen festgelegt, dokumentiert, aktuell gehalten und bei allen Entwicklungsaktivitäten eines Informationssystems angewendet werden.	**X**
8.28	Sichere Kodierung	Bei der Softwareentwicklung müssen die Grundsätze der sicheren Kodierung angewandt werden.	**X**
8.29	Sicherheitsprüfung in Entwicklung und Abnahme	Sicherheitsprüfverfahren müssen definiert und in den Entwicklungslebenszyklus integriert werden.	**X**
8.30	Ausgegliederte Entwicklung	Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgegliederten Systementwicklung leiten, überwachen und überprüfen.	
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	Entwicklungs-, Prüf- und Produktionsumgebungen müssen getrennt und gesichert werden.	**X**
8.32	Änderungssteuerung	Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen müssen Gegenstand von Änderungsmanagementverfahren sein.	**X**
8.33	Informationen zur Prüfung	Die Prüfinformationen müssen in geeigneter Weise ausgewählt, geschützt und verwaltet werden.	**X**
8.34	Schutz der Informationssysteme während der Überwachungsprüfung	Auditprüfungen und andere Sicherheitstätigkeiten, die eine Beurteilung der betrieblichen Systeme beinhalten, müssen zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.	**X**