EPLAN Cloud Plattform ISO/IEC 27001:2013 Erklärung zur Anwendbarkeit

Dokumenteninformation	
Status:	**Freigegeben**
Version:	1.1
Gültigkeit ab:	03.11.2021
Dokumentenart:	ISMS Verfahrensanweisung Anhang
Eigentümer:	Martin Kerkmann
Vertraulichkeitsstufe:	Intern

Freigegebene Version	
Bearbeitungshinweis**:**	Letzte Bearbeitung durch Martin Kerkmann 26.10.2021
Prüfungshinweis:	Geprüft durch Dr. Vincent Layes 03.11.2021
Freigabehinweis**:**	Freigabe durch Dr. Vincent Layes 03.11.2021

Anwendbarkeit von Maßnahmen

Zeitpunkt zum Status der Umsetzung von Maßnahmen: **26.10.2021**

Bedeutung der Abkürzungen in der Spalte „Grund für Auswahl / Ausschluss“

RE: Ergebnisse der Risikoeinschätzung
GVA: Gesetzliche oder vertragliche Anforderungen
EABP: Eigene Anforderung oder beste Praxis
KEM Nicht als erforderliche Maßnahme im Risikobehandlungsplan genannt oder im Gesamtkontext nicht angemessen/geeignet/anwendbar

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.5	**Informationssicherheitsleitlinien**			
A.5.1	Management Informationssicherheitsleitlinien			
A.5.1.1	Ein Satz Informationssicherheitsleitlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.	JA	RE / EABP	Umgesetzt
A.5.1.2	Die Informationssicherheitsleitlinien werden in geplanten Abständen oder jeweils nach geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.	JA	EABP	Umgesetzt
A.6	**Organisation der Informationssicherheit**			
A.6.1	Interne Organisation			
A.6.1.1	Alle Informationssicherheitsverantwortlichkeiten sind festgelegt und zugeordnet.	JA	EABP	Umgesetzt
A.6.1.2	Miteinander in Konflikt stehende Aufgaben und Verantwortungsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.	JA	RE / EABP	Umgesetzt
A.6.1.3	Angemessene Kontakte mit relevanten Behörden werden gepflegt.	JA	EABP	Umgesetzt
A.6.1.4	Angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden werden gepflegt.	JA	EABP	Umgesetzt
A.6.1.5	Informationssicherheit wird im Projektmanagement berücksichtigt, ungeachtet der Art des Projektes.	JA	EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.6.2	Mobilgeräte und Telearbeit			
A.6.2.1	Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sind umgesetzt, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben.	JA	EABP	Umgesetzt
A.6.2.2	Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sind umgesetzt.	JA	EABP	Umgesetzt
A.7	**Personalsicherheit**			
A.7.1	Vor der Beschäftigung			
A.7.1.1	Alle Personen, die sich um eine Beschäftigung bewerben, werden einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.	JA	EABP	Umgesetzt
A.7.1.2	In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sind deren Verantwortlichkeiten und diejenigen der Organisation festgelegt.	JA	EABP	Umgesetzt
A.7.2	Während der Beschäftigung			
A.7.2.1	Die Leitung verlangt von allen Beschäftigten und Auftragnehmern, dass sie die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen.	JA	EABP	Umgesetzt
A.7.2.2	Alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, bekommen ein angemessenes Bewusstsein durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind.	JA	RE / EABP	Umgesetzt, Fortlaufend
A.7.2.3	Ein formal festgelegter und bekanntgegebener Maßregelungsprozess ist eingerichtet, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.	JA	EABP	Umgesetzt
A.7.3	Beendigung oder Änderung der Beschäftigung			
A.7.3.1	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sind festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt.	JA	EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.8	**Verwaltung der Werte**			
A.8.1	Verantwortlichkeit für Werte			
A.8.1.1	Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind erfasst und ein Inventar dieser Werte ist erstellt und wird gepflegt.	JA	EABP	Umgesetzt
A.8.1.2	Für alle Werte, die im Inventar geführt werden, gibt es Zuständige.	JA	EABP	Umgesetzt
A.8.1.3	Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind aufgestellt, dokumentiert und angewendet.	JA	EABP	Umgesetzt
A.8.1.4	Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück.	JA	EABP	Umgesetzt
A.8.2	Informationsklassifizierung			
A.8.2.1	Information ist anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert.	JA	RE / EABP	Umgesetzt
A.8.2.2	Ein angemessener Satz von Verfahren zur Kennzeichnung von Information ist entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.	JA	RE / EABP	Umgesetzt
A.8.2.3	Verfahren für die Handhabung von Werten sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.	JA	RE / EABP	Umgesetzt
A.8.3	Handhabung von Datenträgern			
A.8.3.1	Verfahren für die Handhabung von Wechseldatenträgern sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt	JA	EABP	Umgesetzt
A.8.3.2	Nicht mehr benötigte Datenträger werden sicher und unter Anwendung formaler Verfahren entsorgt.	JA	EABP	Umgesetzt
A.8.3.3	Datenträger, die Information enthalten, sind während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt.	JA	EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.9	**Zugangssteuerung**			
A.9.1	Geschäftsanforderungen an die Zugangssteuerung			
A.9.1.1	Eine Zugangssteuerungsrichtlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft.	JA	RE / EABP	Umgesetzt
A.9.1.2	Benutzer haben ausschließlich Zugang zu denjenigen Netzwerken und Netzwerkdiensten, zu deren Nutzung sie ausdrücklich befugt sind.	JA	RE / EABP	Umgesetzt
A.9.2	Benutzerzugangsverwaltung			
A.9.2.1	Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern ist umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen.	JA	RE / EABP	Umgesetzt
A.9.2.2	Ein formaler Prozess zur Zuteilung von Benutzerzugängen ist umgesetzt, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.	JA	RE / EABP	Umgesetzt
A.9.2.3	Zuteilung und Gebrauch von privilegierten Zugangsrechten ist eingeschränkt und wird gesteuert.	JA	RE / EABP	Umgesetzt
A.9.2.4	Die Zuordnung von geheimer Authentisierungsinformation wird über einen formalen Verwaltungsprozess gesteuert.	JA	RE / EABP	Umgesetzt
A.9.2.5	Die für Werte Zuständigen überprüfen in regelmäßigen Abständen die Benutzerzugangsrechte.	JA	RE / EABP	Umgesetzt
A.9.2.6	Die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen werden bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst.	JA	RE / EABP	Umgesetzt
A.9.3	Benutzerverantwortlichkeiten			
A.9.3.1	Benutzer sind verpflichtet, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen.	JA	RE / EABP	Umgesetzt
A.9.4	Zugangssteuerung für Systeme und Anwendungen			
A.9.4.1	Zugang zu Information und Anwendungssystemfunktionen ist entsprechend der Zugangssteuerungsrichtlinie eingeschränkt.	JA	RE / EABP	Umgesetzt
A.9.4.2	Soweit es die Zugangssteuerungsrichtlinie erfordert, wird der Zugang zu Systemen und Anwendungen durch ein sicheres Anmeldeverfahren gesteuert.	JA	RE / EABP	Umgesetzt
A.9.4.3	Systeme zur Verwaltung von Kennwörtern sind interaktiv sein und stellen starke Kennwörter sicher.	JA	RE / EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.9.4.4	Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.	JA	EABP	Umgesetzt
A.9.4.5	Zugang zu Quellcode von Programmen ist eingeschränkt.	JA	EABP	Umgesetzt
A.10	**Kryptographie**			
A.10.1	Kryptographische Maßnahmen			
A.10.1.1	Eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information ist entwickelt und umgesetzt.	JA	RE / EABP	Umgesetzt
A.10.1.2	Eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln ist entwickelt und wird über deren gesamten Lebenszyklus umgesetzt.	JA	RE / EABP	Umgesetzt
A.11	**Physische und umgebungsbedingte Sicherheit**			
A.11.1	Sicherheitsbereiche			
A.11.1.1	Zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitsperimeter festgelegt und werden verwendet.	JA	EABP	Umgesetzt
A.11.1.2	Sicherheitsbereiche sind durch eine angemessene Zutrittssteuerung geschützt, um sicherzustellen, dass nur berechtigtes Personal Zugang hat.	JA	EABP	Umgesetzt
A.11.1.3	Die physische Sicherheit für Büros, Räume und Einrichtungen ist konzipiert und wird angewendet.	JA	EABP	Umgesetzt
A.11.1.4	Physischer Schutz vor Naturkatastrophen, bösartigen Angriffen oder Unfällen ist konzipiert und wird angewendet.	JA	EABP	Umgesetzt
A.11.1.5	Verfahren für das Arbeiten in Sicherheitsbereichen sind konzipiert und werden angewendet.	JA	EABP	Umgesetzt
A.11.1.6	Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, werden überwacht und sind, falls möglich, von informationsverarbeitenden Einrichtungen getrennt, um unbefugten Zutritt zu verhindern.	JA	EABP	Umgesetzt
A.11.2	Geräte und Betriebsmittel			
A.11.2.1	Geräte und Betriebsmittel sind so platziert und geschützt, dass Risiken durch umweltbedingte Bedrohungen und Gefahren sowie Möglichkeiten des unbefugten Zugangs verringert sind.	JA	EABP	Umgesetzt
A.11.2.2	Geräte und Betriebsmittel sind vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt.	JA	EABP	Umgesetzt
A.11.2.3	Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, und die Stromverkabelung sind vor Unterbrechung, Störung oder Beschädigung geschützt.	JA	EABP	Umgesetzt
A.11.2.4	Geräte und Betriebsmittel werden ordnungsgemäß Instand gehalten, um ihre fortgesetzte Verfügbarkeit und Integrität sicherzustellen.	JA	EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.11.2.5	Geräte, Betriebsmittel, Information oder Software werden nicht ohne vorherige Genehmigung vom Betriebsgelände entfernt.	JA	EABP	Umgesetzt
A.11.2.6	Werte außerhalb des Standorts werden gesichert, um die verschiedenen Risiken beim Betrieb außerhalb der Räumlichkeiten der Organisation zu berücksichtigen.	JA	EABP	Umgesetzt
A.11.2.7	Alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, werden überprüft, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.	JA	EABP	Umgesetzt
A.11.2.8	Benutzer stellen sicher, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt sind.	JA	EABP	Umgesetzt
A.11.2.9	Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren für informationsverarbeitende Einrichtungen werden angewendet.	JA	EABP	Umgesetzt
A.12	**Betriebssicherheit**			
A.12.1	Betriebsabläufe und -verantwortlichkeiten			
A.12.1.1	Die Bedienabläufe sind dokumentiert und allen Benutzern, die sie benötigen, zugänglich.	JA	EABP	Umgesetzt
A.12.1.2	Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen werden gesteuert.	JA	EABP	Umgesetzt
A.12.1.3	Die Ressourcennutzung/Benutzung von Ressourcen wird überwacht und abgestimmt, und es werden Prognosen zu zukünftigen Kapazitätsanforderungen erstellt, um die erforderliche Systemleistung sicherzustellen.	JA	RE / EABP	Umgesetzt
A.12.1.4	Entwicklungs-, Test- und Betriebsumgebungen sind voneinander getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.	JA	EABP	Umgesetzt
A.12.2	Schutz vor Schadsoftware			
A.12.2.1	Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer sind umgesetzt.	JA	RE / EABP	Umgesetzt
A.12.3	Datensicherung			
A.12.3.1	Sicherheitskopien von Information, Software und Systemabbildern werden entsprechend einer vereinbarten Sicherungsrichtlinie angefertigt und regelmäßig getestet.	JA	RE / EABP	Umgesetzt
A.12.4	Protokollierung und Überwachung			
A.12.4.1	Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, werden erzeugt, aufbewahrt und regelmäßig überprüft.	JA	EABP	Umgesetzt
A.12.4.2	Protokollierungseinrichtungen und Protokollinformation sind vor Manipulation und unbefugtem Zugriff geschützt.	JA	EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.12.4.3	Tätigkeiten von Systemadministratoren und Systembedienern werden aufgezeichnet und die Protokolle sind geschützt und werden regelmäßig überprüft.	JA	EABP	Umgesetzt
A.12.4.4	Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder eines Sicherheitsbereichs werden mit einer einzigen Referenzzeitquelle synchronisiert.	JA	EABP	Umgesetzt
A.12.5	Steuerung von Software im Betrieb			
A.12.5.1	Verfahren zur Steuerung der Installation von Software auf Systemen im Betrieb sind umgesetzt.	JA	EABP	Umgesetzt
A.12.6	Handhabung technischer Schwachstellen			
A.12.6.1	Information über technische Schwachstellen verwendeter Informationssysteme wird rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen wird bewertet und angemessene Maßnahmen werden ergriffen, um das dazugehörige Risiko zu behandeln.	JA	RE / EABP	Umgesetzt
A.12.6.2	Regeln für die Softwareinstallation durch Benutzer sind festgelegt und umgesetzt.	JA	EABP	Umgesetzt
A.12.7	Audit von Informationssystemen			
A.12.7.1	Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systeme beinhalten, werden sorgfältig geplant und vereinbart, um Störungen der Geschäftsprozesse zu minimieren.	JA	RE / EABP	Umgesetzt
A.13	**Kommunikationssicherheit**			
A.13.1	Netzwerksicherheitsmanagement			
A.13.1.1	Netzwerke werden verwaltet und gesteuert, um Information in Systemen und Anwendungen zu schützen.	JA	EABP	Umgesetzt
A.13.1.2	Sicherheitsmechanismen, Dienstgüte und Anforderungen an die Verwaltung aller Netzwerkdienste sind bestimmt und werden sowohl für interne als auch für ausgegliederte Netzwerkdienste in Vereinbarungen aufgenommen.	JA	EABP	Umgesetzt
A.13.1.3	Informationsdienste, Benutzer und Informationssysteme in Netzwerken werden gruppenweise voneinander getrennt gehalten.	JA	EABP	Umgesetzt
A.13.2	Informationsübertragung			
A.13.2.1	Formale Übertragungsrichtlinien, Verfahren und Maßnahmen sind vorhanden, um die Übertragung von Information für alle Arten von Kommunikationseinrichtungen zu schützen.	JA	RE / EABP	Umgesetzt
A.13.2.2	Vereinbarungen behandeln die sichere Übertragung von Geschäftsinformation zwischen der Organisation und externen Parteien.	JA	EABP	Umgesetzt
A.13.2.3	Information in der elektronischen Nachrichtenübermittlung ist angemessen geschützt.	JA	EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.13.2.4	Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, werden identifiziert, regelmäßig überprüft und sind dokumentiert.	JA	EABP	Umgesetzt
A.14	**Anschaffung, Entwicklung und Instandhalten von Systemen**			
A.14.1	Sicherheitsanforderungen für Informationssysteme			
A.14.1.1	Die Anforderungen, die sich auf Informationssicherheit beziehen, sind in die Anforderungen an neue Informationssysteme oder die Verbesserungen bestehender Informationssysteme aufgenommen.	JA	EABP	Umgesetzt
A.14.1.2	Information, die durch Anwendungsdiensten über öffentliche Netzwerke übertragen wird, ist vor betrügerischer Tätigkeit, Vertragsstreitigkeiten und unbefugter Offenlegung sowie Veränderung geschützt.	JA	EABP	Umgesetzt
A.14.1.3	Information, die an Transaktionen bei Anwendungsdiensten beteiligt ist, ist so geschützt, dass unvollständige Übertragung, Fehlleitung, unbefugte Offenlegung, unbefugte Vervielfältigung oder unbefugte Wiederholung von Nachrichten verhindert ist.	JA	EABP	Umgesetzt
A.14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen			
A.14.2.1	Regeln für die Entwicklung von Software und Systemen sind festgelegt und bei Entwicklungen innerhalb der Organisation angewendet.	JA	RE / EABP	Umgesetzt
A.14.2.2	Änderungen an Systemen innerhalb des Entwicklungszyklus werden durch formale Verfahren zur Verwaltung von Änderungen gesteuert.	JA	EABP	Umgesetzt
A.14.2.3	Bei Änderungen an Betriebsplattformen, werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationstätigkeiten oder Organisationssicherheit gibt.	JA	EABP	Umgesetzt
A.14.2.4	Änderungen an Softwarepaketen werden nicht gefördert, sind auf das Erforderliche beschränkt und alle Änderungen unterliegen einer strikten Steuerung.	JA	EABP	Umgesetzt
A.14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sind festgelegt, dokumentiert, werden aktuell gehalten und bei jedem Umsetzungsvorhaben eines Informationssystems angewendet.	JA	EABP	Umgesetzt
A.14.2.6	Organisationen schaffen sichere Entwicklungsumgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus und schützen diese angemessen.	JA	EABP	Umgesetzt
A.14.2.7	Die Organisation beaufsichtigt und überwacht die Tätigkeit ausgegliederter Systementwicklung.	JA	EABP	Umgesetzt
A.14.2.8	Die Sicherheitsfunktionalität wird während der Entwicklung getestet.	JA	EABP	Umgesetzt
A.14.2.9	Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt.	JA	EABP	Umgesetzt
A.14.3	Testdaten			

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.14.3.1	Testdaten werden sorgfältig ausgewählt, geschützt und gesteuert.	JA	EABP	Umgesetzt
A.15	**Lieferantenbeziehungen**			
A.15.1	Informationssicherheit in Lieferantenbeziehungen			
A.15.1.1	Die Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation werden mit dem Zulieferer vereinbart und sind dokumentiert.	JA	EABP	Umgesetzt
A.15.1.2	Alle relevanten Informationssicherheitsanforderungen werden mit jedem Lieferanten, der Zugang zu Information der Organisation haben könnte, diese verarbeiten, speichern, weitergeben könnte oder IT-Infrastrukturkomponenten dafür bereitstellt, festgelegt und sind vereinbart.	JA	EABP	Umgesetzt
A.15.1.3	Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, werden in Vereinbarungen mit Lieferanten aufgenommen.	JA	EABP	Umgesetzt
A.15.2	Steuerung der Dienstleistungserbringung von Lieferanten			
A.15.2.1	Organisationen überwachen, überprüfen und auditieren die Dienstleistungserbringung durch Lieferanten regelmäßig.	JA	EABP	Umgesetzt
A.15.2.2	Änderungen bei der Bereitstellung von Dienstleistungen durch Lieferanten werden gesteuert. Solche Änderungen umfassen auch die Pflege und Verbesserung bestehender Informationssicherheitsrichtlinien, -Verfahren und Maßnahmen. Dabei werden die Kritikalität der betroffenen Geschäftsinformation, -systeme und -prozesse und eine erneute Risikobeurteilung beachtet.	Ja	EABP	Umgesetzt
A.16	Handhabung von Informationssicherheitsvorfällen			
A.16.1	Handhabung von Informationssicherheitsvorfällen und Verbesserungen			
A.16.1.1	Handhabungsverantwortlichkeiten und -verfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen.	Ja	RE / EABP	Umgesetzt
A.16.1.2	Informationssicherheitsereignisse werden so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet.	Ja	RE / EABP	Umgesetzt
A.16.1.3	Beschäftigte und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, werden angehalten, jegliche beobachteten oder vermuteten Schwächen in der Informationssicherheit in Systemen oder Diensten festzuhalten und zu melden.	Ja	RE / EABP	Umgesetzt
A.16.1.4	Informationssicherheitsereignisse werden beurteilt, und es wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind.	Ja	RE / EABP	Umgesetzt
A.16.1.5	Auf Informationssicherheitsvorfälle wird entsprechend den dokumentierten Verfahren reagiert.	Ja	RE / EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.16.1.6	Aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse werden dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.	Ja	RE / EABP	Umgesetzt
A.16.1.7	Die Organisation legt Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, fest und wendet diese an.	Ja	RE / EABP	Umgesetzt
A.17	Informationssicherheitsaspekte beim Business Continuity Management			
A.17.1	Aufrechterhalten der Informationssicherheit			
A.17.1.1	Die Organisation bestimmt ihre Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements bei widrigen Situationen, z. B. Krise oder Katastrophe.	Ja	RE / EABP	Umgesetzt
A.17.1.2	Die Organisation legt Prozesse, Verfahren und Maßnahmen fest, dokumentiert, setzt sie um und erhält diese aufrecht, um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können.	Ja	RE / EABP	Umgesetzt
A.17.1.3	Die Organisation überprüft in regelmäßigen Abständen die festgelegten und umgesetzten Maßnahmen zur Aufrechterhaltung der Informationssicherheit, um sicherzustellen, dass diese gültig und in widrigen Situationen wirksam sind.	Ja	RE / EABP	Umgesetzt
A.17.2	Redundanzen			
A.17.2.1	Informationsverarbeitende Einrichtungen werden mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert.	Ja	RE / EABP	Umgesetzt
A.18	**Compliance**			
A.18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen			
A.18.1.1	Alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen der Organisation zur Einhaltung dieser Anforderungen sind für jedes Informationssystem und die Organisation ausdrücklich bestimmt und dokumentiert und werden auf dem neuesten Stand gehalten.	Ja	EABP	Umgesetzt
A.18.1.2	Es sind angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und die Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.	Ja	EABP	Umgesetzt
A.18.1.3	Aufzeichnungen sind gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt.	Ja	EABP	Umgesetzt
A.18.1.4	Die Privatsphäre und der Schutz von personenbezogener Information sind, soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt.	Ja	RE / EABP	Umgesetzt

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit	Grund für Auswahl / Ausschluss	Status
A.18.1.5	Kryptographische Maßnahmen werden unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt.	Ja	RE / EABP	Umgesetzt
A.18.2	Überprüfungen der Informationssicherheit			
A.18.2.1	Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung (d. h. Maßnahmenziele, Maßnahmen, Richtlinien, Prozesse und Verfahren zur Informationssicherheit) werden auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft.	Ja	EABP	Umgesetzt
A.18.2.2	Leitende Angestellte überprüfen regelmäßig die Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien, Standards und jeglicher sonstiger Sicherheitsanforderungen bei der Informationsverarbeitung und den Verfahren in ihrem Verantwortungsbereich.	Ja	EABP	Umgesetzt
A.18.2.3	Informationssysteme werden regelmäßig auf Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation überprüft.	Ja	RE / EABP	Umgesetzt