Statement of Applicability

Erklärung der Anwendbarkeit

evocenta
digital intelligent interactions

Stand: 10.02.2022

ISO/IEC 27001:2013 Anhang A Maßnahmen		Angewandt?	Gründe für Einschluss ABP	RM	G	V
Sek.	**Kontrollelement**					
5	**Informationssicherheitsrichtlinien**					
5,1	**Vorgaben der Leitung für Informationssicherheit**					
	Ziel: Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in					
5.1.1	Informationssicherheitsrichtlinie	Ja	x			x
5.1.2	Überprüfung der Informationssicherheitsrichtlinien	Ja	x			x
6	**Organisation der Informationssicherheit**					
6,1	**Interne Organisation**					
	Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der					
6.1.1	Informationssicherheitsrollen/Verantwortlichkeiten	Ja	x	x		
6.1.2	Aufgabentrennung	Ja	x			
6.1.3	Kontakt mit Behörden	Ja		x	x	
6.1.4	Kontakt mit speziellen Interessensgruppen	Ja	x	x		
6.1.5	Security im Projektmanagement	Ja	x	x		
6,2	**Mobilgeräte und Telearbeit**					
	Ziel: Die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt.					
6.2.1	Richtlinie zu Mobilgeräten	Ja	x	x		
6.2.2	Telearbeit	Ja		x	x	
7	**Personalsicherheit**					
7,1	**Vor der Beschäftigung**					
	Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen					
7.1.1	Sicherheitsüberprüfung	Ja	x			
7.1.2	Beschäftigungs- und Vertragsbedingungen	Ja			x	
7,2	**Während der Beschäftigung**					
	Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer sich ihrer Verantwortlichkeiten					
7.2.1	Verantwortlichkeiten der Leitung	Ja		x		
7.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Ja	x	x		
7.2.3	Maßregelungsprozess	Ja	x	x		
7,3	**Beendigung und Änderung der Beschäftigung**					
	Ziel: Der Schutz der Interessen der Organisation ist Teil des Prozesses der Änderung oder					
7.3.1	Verantwortlichkeit bei Beendigung oder Änderung der Beschäftigung	Ja		x		
8	**Verwaltung der Werte**					
8,1	**Verantwortlichkeit für Werte**					
	Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem					

Legende	
Kontrollelement angewendet?	
Ja	Kontrollelement umgesetzt und aktiv
Nein	Kontrollelement nicht umgesetzt
N/A	Kontrollelement ist nicht anwendbar

Key driver	
G	Gesetzliche Anforderung
V	Vertragliche Verpflichtung
RM	Business-Entscheidung nach Risikoabwägung
ABP	Adopted best practice
N/A	Nicht anwendbar

8.1.1	Inventarisierung der Werte	Ja	x	x		
8.1.2	Zuständigkeit für Werte	Ja		x		
8.1.3	Zulässiger Gebrauch von Werten	Ja	x	x		
8.1.4	Rückgabe von Werten	Ja	x	x		
8,2	**Informationsklassifizierung**					
	Ziel: Es ist sichergestellt, dass Information ein angemessenes Schutzniveau entsprechend ihrer					
8.2.1	Klassifizierung von Informationen	Ja	x	x	x	
8.2.2	Kennzeichnung von Informationen	Ja	x	x		
8.2.3	Handhabung von Werten	Ja	x	x	x	
8,3	**Handhabung von Datenträgern**					
	Ziel: Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information, die auf					
8.3.1	Handhabung von Wechseldatenträgern	Ja		x		
8.3.2	Entsorgung von Datenträgern	Ja		x		
8.3.3	Transport von Datenträgern	Ja		x		
9	**Zugangssteuerung**					
9,1	**Geschäftsanforderungen an die Zugangsteuerung**					
	Ziel: Der Zugang zu Informationen und informationsverarbeitenden Einrichtungen ist eingeschränkt.					
9.1.1	Zugangssteuerungsrichtlinie	Ja	x	x		
9.1.2	Zugang zu Netzwerken und Netzwerkdiensten	Ja	x	x		
9,2	**Benutzerzugangsverwaltung**					
	Ziel: Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und					
9.2.1	Registrierung und Deregistrierung von Benutzern	Ja	x	x		
9.2.2	Zuteilung von Benutzerzugängen	Ja	x	x		
9.2.3	Verwaltung privilegierter Zugangsrechte	Ja	x	x		
9.2.4	Verwaltung geheimer Authentisierungsinformationen von Benutzern	Ja	x	x		
9.2.5	Überprüfung von Zugangsrechten	Ja	x	x		
9.2.6	Entzug oder Anpassung von Zugangsrechten	Ja	x	x		
9,3	**Benutzerverantwortlichkeiten**					
	Ziel: Benutzer sind für den Schutz Ihrer Authentisierungsinformation verantwortlich gemacht.					
9.3.1	Gebrauch geheimer Authentisierungsinformation	Ja	x	x		
9,4	**Zugangssteuerung für Systeme und Anwendungen**					
	Ziel: Unbefugter Zugang zu Systemen und Anwendungen ist unterbunden.					
9.4.1	Informationszugangsbeschränkung	Ja	x	x		
9.4.2	Sichere Anmeldeverfahren	Ja	x	x		
9.4.3	System zur Verwaltung von Kennwörtern	Ja	x	x		
9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Ja		x		
9.4.5	Zugangssteuerung für Quellcode von Programmen	Ja	x	x		
10	**Kryptographie**					
10,1	**Kryptographische Maßnahmen**					

	Ziel: Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit,					
10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	Ja	x	x		
10.1.2	Schlüsselverwaltung	Ja	x	x		
11	**Physische und umgebungsbezogene Sicherheit**					
11,1	**Sicherheitsbereiche**					
	Ziel: Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Information und informations-					
11.1.1	Physischer Sicherheitsperimeter	Ja	x	x		
11.1.2	Physische Zutrittssteuerung	Ja	x	x		
11.1.3	Sichern von Büros, Räumen und Einrichtungen	Ja	x	x		
11.1.4	Schutz vor externen und umweltbedingten Bedrohungen	Ja	x	x		
11.1.5	Arbeiten in Sicherheitsbereichen	Ja	x	x		
11.1.6	Anlieferungs- und Ladebereiche	Ja	x	x		
11,2	**Geräte und Betriebsmittel**					
	Ziel: Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von					
11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln	Ja	x	x		
11.2.2	Versorgungseinrichtungen	Ja	x	x		
11.2.3	Sicherheit der Verkabelung	Ja	x	x		
11.2.4	Instandhalten von Geräten und Betriebsmitteln	Ja	x	x		
11.2.5	Entfernen von Werten	Ja	x	x		
11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	Ja	x	x		
11.2.7	Sichere Entsorgung oder Wiederherstellung von Geräten und Betriebsmitteln	Ja	x	x		
11.2.8	Unbeaufsichtigte Benutzergeräte	Ja	x	x		
11.2.9	Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	Ja	x	x		
12	**Betriebssicherheit**					
12,1	**Betriebsabläufe und –verantwortlichkeiten**					
	Ziel: Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist					
12.1.1	Dokumentierte Betriebsabläufe	Ja	x	x		
12.1.2	Änderungssteuerung	Ja	x	x		
12.1.3	Kapazitätssteuerung	Ja	x	x		
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	Ja	x	x		
12,2	**Schutz vor Schadsoftware**					
	Ziel: Information und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.					
12.2.1	Maßnahmen gegen Schadsoftware	Ja	x	x		
12,3	**Backup**					
	Ziel: Daten sind vor Verlust geschützt.					
12.3.1	Sicherung von Information	Ja	x	x		
12,4	**Protokollierung und Überwachung**					

	Ziel: Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.					
12.4.1	Ereignisprotokollierung	Ja	x	x		
12.4.2	Schutz der Protokollinformation	Ja	x	x		
12.4.3	Administratoren- und Bedienerprotokolle	Ja		x		
12.4.4	Uhrensynchronisation	Ja	x	x		
12,5	**Steuerung von Software im Betrieb**					
	Ziel: Die Integrität von Systemen im Betrieb ist sichergestellt.					
12.5.1	Installation von Software auf Systemen im Betrieb	Ja	x	x		
12,6	**Handhabung technischer Schwachstellen**					
	Ziel: Die Ausnutzung technischer Schwachstellen ist verhindert.					
12.6.1	Handhabung von technischen Schwachstellen	Ja	x	x		
12.6.2	Einschränkung von Softwareinstallation	Ja	x	x		
12,7	**Audits von Informationssystemen**					
	Ziel: Die Auswirkung von Audittätigkeiten auf Systeme im Betrieb ist minimiert.					
12.7.1	Maßnahmen für Audits von Informationssystemen	Ja	x			
13	**Kommunikationssicherheit**					
13,1	**Netzwerksicherheitsmanagement**					
	Ziel: Der Schutz von Information in Netzwerken und den unterstützenden informationsverarbeitenden					
13.1.1	Netzwerksteuerungsmaßnahmen	Ja	x	x		
13.1.2	Sicherheit von Netzwerkdiensten	Ja	x	x		
13.1.3	Trennung in Netzwerken	Ja	x	x		x
13,2	**Informationsübertragung**					
	Ziel: Die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit					
13.2.1	Richtlinien und Verfahren zur Informationsübertragung	Ja				
13.2.2	Vereinbarungen zur Informationsübertragung	Ja				
13.2.3	Elektronische Nachrichtenübermittlung	Ja				
13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Ja		x	x	x
14	**Anschaffung, Entwicklung und Instandhaltung von Systemen**					
14,1	**Sicherheitsanforderungen an Informationssysteme**					
	Ziel: Es ist sichergestellt, dass Informationssicherheit ein fester Bestandteil über den gesamten					
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	Ja	x	x		
14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	Ja	x	x		
14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	Ja	x	x		
14,2	**Sicherheit in Entwicklungs- und Unterstützungsprozessen**					
	Ziel: Es ist sichergestellt, dass Informationssicherheit im Entwicklungszyklus von Informationssystemen					
14.2.1	Richtlinie für sichere Entwicklung	Ja	x	x		
14.2.2	Verfahren zur Verwaltung von Systemänderungen	Ja	x	x		

14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	Ja	x	x		
14.2.4	Beschränkung von Änderungen an Softwarepaketen	Ja	x	x		
14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	Ja	x	x		
14.2.6	Sichere Entwicklungsumgebung	Ja	x	x		
14.2.7	Ausgegliederte Entwicklung	Ja	x	x		
14.2.8	Testen der Systemsicherheit	Ja	x	x		
14.2.9	Systemabnahmetest	Ja	x	x		
14,3	**Testdaten**					
	Ziel: Der Schutz von Daten, die für das Testen verwendet werden, ist sichergestellt.					
14.3.1	Schutz von Testdaten	Ja		x	x	
15	**Lieferantenbeziehungen**					
15,1	**Informationssicherheit in Lieferantenbeziehungen**					
	Ziel: Für Lieferanten zugängliche Werte des Unternehmens sind geschützt.					
15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	Ja		x		
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	Ja		x		x
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie	Ja		x		
15,2	**Steuerung der Dienstleistungserbringung von Lieferanten**					
	Ziel: Ein vereinbartes Niveau der Informationssicherheit und der Dienstleistungserbringung ist im					
15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen	Ja		x		
15.2.2	Handhabung der Änderungen von	Ja		x		
16	**Handhabung von Informationssicherheitsvorfällen**					
16,1	**Handhabung von Informationssicherheitsvorfällen und –verbesserungen**					
	Ziel: Eine konsistente und wirksame Herangehensweise für die Handhabung von					
16.1.1	Verantwortlichkeiten und Verfahren	Ja	x	x		
16.1.2	Meldung von Informationssicherheitsereignissen	Ja	x	x	x	x
16.1.3	Meldung von Schwächen in der Informationssicherheit	Ja	x	x		
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	Ja	x	x		
16.1.5	Reaktion auf Informationssicherheitsvorfälle	Ja	x	x		
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	Ja	x	x		
16.1.7	Sammeln von Beweismaterial	Ja	x	x	x	
17	**Informationssicherheitsaspekte beim Business Continuity Management**					
17,1	**Aufrechterhalten der Informationssicherheit**					
	Ziel: Die Aufrechterhaltung der Informationssicherheit sollte in das Business Continuity Management-					
17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit	Ja	x	x		
17.1.2	Umsetzen der Aufrechterhaltung der Informationssicherheit	Ja	x	x		
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	Ja	x	x		

17,2	**Redundanzen**					
	Ziel: Die Verfügbarkeit von informationsverarbeitenden Einrichtungen ist sichergestellt.					
17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	Ja	x	x		
18	**Compliance**					
18,1	**Einhaltung gesetzlicher und vertraglicher Anforderungen**					
	Ziel: Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit					
18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	Ja	x	x	x	x
18.1.2	Geistige Eigentumsrechte	Ja	x		x	
18.1.3	Schutz von Aufzeichnungen	Ja	x	x	x	x
18.1.4	Privatsphäre und Schutz von personenbezogener Information	Ja			x	
18.1.5	Regelungen bezüglich kryptographischer Maßnahmen	Ja			x	
18,2	**Überprüfungen der Informationssicherheit**					
	Ziel: Informationssicherheit ist in Übereinstimmung mit den Richtlinien und Verfahren der Organisation					
18.2.1	Unabhängige Überprüfung der Informationssicherheit	Ja	x			x
18.2.2	Einhaltung von Sicherheitsrichtlinien und Standards	Ja	x			x
18.2.3	Überprüfung der Einhaltung von technischen Vorgaben	Ja	x			x