Statement of Applicability

Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023

Inhaltsverzeichnis

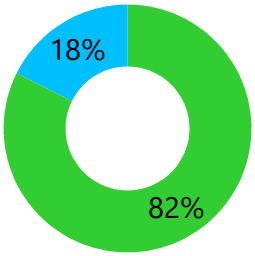
ISO/IEC 27001:2022

Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023

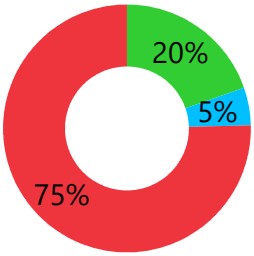
Stand:	31.01.2024
Beschreibung:	Diese Norm ist für alle Organisationsarten anwendbar und legt die Anforderungen an Aufstellen, Umsetzen, Betrieb, Überwachung, Bewertung, Wartung und Verbesserung von dokumentierten Informationssicherheit-Managementsystemen in Bezug auf die allgemeinen Geschäftsrisiken einer Organisation fest. Sie legt außerdem die Anforderungen an die Einführung von Sicherheitskontrollen fest, die auf die Bedürfnisse einer Organisation oder Teilen davon zugeschnitten sind. Das Informationssicherheits-Managementsystem ist dafür entwickelt worden, die Auswahl ausreichender und angemessener Sicherheitskontrollen zu gewährleisten, die den Informationsbestand sichern und interessierten Partnern Vertrauenswürdigkeit vermitteln.
Geltungsbereich:	Der Geltungsbereich des ISMS erstreckt sich auf alle iteratec-Standorte: - München - Hamburg - Stuttgart - Frankfurt - Düsseldorf - Wien - Wrocław (Breslau) Dabei sind folgenden Standorte explizit zertifiziert nach ISO 27001: - München - Hamburg - Stuttgart - Frankfurt - Düsseldorf Das ISMS umfasst die Geschäftsprozesse der folgenden Themenfelder der iteratec und LUY und alle dort tätigen internen und externen Mitarbeiter und Dienstleister: "Betrieb eigener Systeme (Unterstützender Prozess der iteratec und LUY) zur Unternehmensführung und -Verwaltung" "Softwareentwicklung, IT-Beratung und Betrieb im Kundenauftrag und Produktentwicklung und -Betrieb", soweit dafür Systeme und Infrastruktur der iteratec und LUY verwendet werden

Maßnahmen Übersicht

34 Maßnahmen für diesen Geltungsbereich sind diesem Standard bzw. dieser Norm zugewiesen.



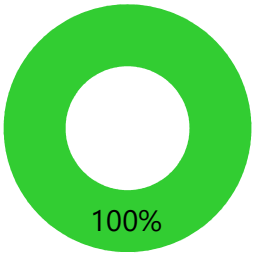
Maßnahmen:
- Erledigt (28/34)
- Offen (6/34)



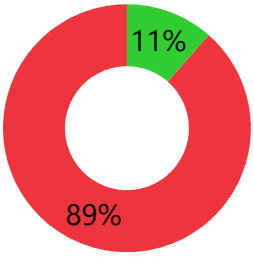
Kapitel:
- mit erledigten Maßnahmen (24/122)
- mit offenen Maßnahmen (6/122)
- ohne Maßnahmen (92/122)

Kontrollübersicht

14 Kontrollen für diesen Geltungsbereich sind diesem Standard bzw. dieser Norm zugewiesen.



Durchführungen:
- Erfolgreich (7/7)



Kapitel:
- mit aktiven Kontrollen (14/122)
- ohne Kontrollen (108/122)

Relevanz nach Kapiteln

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
04	**Kontext der Organisation**		Ja	Legende für "Begründung" - G: gesetzliche Anforderung - V: vertragliche Verpflichtung - B: Anforderung aus Geschäftsprozessen (Business) bzw. der beteiligten Parteien - R: Aufgrund der Risikobewertung
4.1	Verstehen der Organisation und ihres Kontextes	M_046 OFI #1 Dokumentation Schnittstelle ISMS-intern zu ISMS-zertifiziert	Ja	
4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien		Ja	
4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystem	M_074 Prüfung des Einsatzes Lieferantenmanagement-Modues von HitGuard	Ja	
4.4	Informationssicherheitsmanagementsystem		Ja	
05	**Führung**		Ja	
5.1	Führung und Verpflichtung	K_011 Überprüfung der Informations-sicherheitsrichtlinien	Ja	
5.2	Politik	M_047 OFI #5 Verständlichere und realistischere Spezifizierung der Sicherheitsziele	Ja	
5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	M_004 Aktualisierung der Rollen und Rechte im ISMS	Ja	
06	**Planung**		Ja	

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
6.1	Maßnahmen zum Umgang mit Risiken und Chancen	M_051 OFI #10 Sicherstellen von Synchronität zwischen Risikotabelle und Confluence	Ja	
6.1.1	Allgemeines	M_051	Ja	
6.1.2	Informationssicherheitsrisikobeurteilung	M_051	Ja	
6.1.3	Informationssicherheitsrisikobehandlung	M_051	Ja	
6.2	Informationssicherheitsziele und Planung zu deren Erreichung	M_072 Aktualisierung der definierten ISMS-KPI, K_012 Informationssicherheitsbewusstsein, -ausbildung und -schulung	Ja	
07	**Unterstützung**		Ja	
7.1	Ressourcen		Ja	
7.2	Kompetenz		Ja	
7.3	Bewusstsein		Ja	
7.4	Kommunikation	M_048 OFI #6 Dokumentation der Außenkommunikation	Ja	
7.5	Dokumentierte Information		Ja	
7.5.1	Allgemeines		Ja	
7.5.2	Erstellen und Aktualisieren	M_009 Aktualisierung des Comala-Plugins in allen Confluance Richtlinien, M_010 Abnahme der ISMS Leit- und Richtlinien, K_001 Erstellen und Aktualisieren (von Dokumenten)	Ja	
7.5.3	Lenkung dokumentierter Information		Ja	
08	**Betrieb**		Ja	
8.1	Betriebliche Planung und Steuerung		Ja	

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
8.2	Informationssicherheitsrisikobeurteilung	M_011 Informationssicherheitsrisikobeurteilun regelmäßig erstellen	Ja	
8.3	Informationssicherheitsrisikobehandlung		Ja	
09	**Bewertung der Leistung**		Ja	
9.1	Überwachung, Messung, Analyse und Bewertung	K_008 Messung der Wirksamkeit	Ja	
9.2	Internes Audit	K_009 Internes Audit	Ja	
9.2.1	Allgemeines	K_009	Ja	
9.2.2	Internes Auditprogramm	K_009	Ja	
9.3	Managementbewertung	K_010 Managementbewertung	Ja	
9.3.1	Allgemeines	K_010	Ja	
9.3.2	Inputs der Managementbewertung	K_010	Ja	
9.3.3	Ergebnisse der Managementbewertung	K_010	Ja	
10	**Verbesserung**		Ja	
10.1	Fortlaufende Verbesserung		Ja	
10.2	Nichtkonformität und Korrekturmaßnahmen		Ja	
A.5	**Organisatorische Maßnahmen**		Ja	
A.5.1	Informationssicherheitsrichtlinien		Ja	V, B, R
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten		Ja	B, R
A.5.3	Aufgabentrennung		Ja	G, B, R
A.5.4	Verantwortlichkeiten der Leitung		Ja	B, R
A.5.5	Kontakt mit Behörden		Ja	G, B, R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.5.6	Kontakt mit speziellen Interessensgruppen		Ja	B, R
A.5.7	Bedrohungsintelligenz		Ja	B, R
A.5.8	Informationssicherheit im Projektmanagement	M_012 Verbesserung der Verankerung Security in den Projekten, M_044 ABW #2 Abweichung Sichere SW Entwicklung in Projekten, M_045 OFI #4 Sicherheit im Produkt	Ja	V, B, R
A.5.9	Inventar der Informationen und anderen damit verbundenen Werten	M_013 Initiale Befüllung der Assets in HitGuard, M_037 ABW #1 Abweichung Assetmanagement, M_049 OFI #8 Dokumentation der Verortung von Kundendaten in den Primary Assets, M_050 OFI #9 Überlegung zur Nachvollziehbarkeit der Bildung von Assetgruppen, M_051 OFI #10 Sicherstellen von Synchronität zwischen Risikotabelle und Confluence, M_052 OFI #11 Vereinfachung des Assetmanagement, M_053 OFI #12 Bewertung der Nützlichkeit von eigenen Assetgruppen für IOTs	Ja	B, R
A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten		Ja	B, R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.5.11	Rückgabe von Werten		Ja	B, R
A.5.12	Klassifizierung von Information		Ja	B, R
A.5.13	Kennzeichnung von Information		Ja	B, R
A.5.14	Informationsübertragung		Ja	R
A.5.15	Zugangssteuerung	M_014 OFI #15 Überprüfung von BYOD-Risiko und -Maßnahmen	Ja	B, R
A.5.16	Identitätsmanagement		Ja	B, R
A.5.17	Informationen zur Authentifizierung		Ja	V, B, R
A.5.18	Zugangsrechte	K_002 Überprüfung von Benutzerzugangsrechten, K_023 Überprüfung von Benutzerzugangsrechten in EntraID	Ja	B, R
A.5.19	Informationssicherheit in Lieferantenbeziehungen	M_015 Verbesserung der Lieferantenprüfung	Ja	B, R
A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen		Ja	B, R
A.5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette		Ja	B, R
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	K_014 Überwachung und Überprüfung von Lieferantendienstleistungen	Ja	B, R
A.5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	M_016 Konzept für den Ausstieg aus Cloud-Diensten	Ja	B, R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen		Ja	B, R
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse		Ja	B, R
A.5.26	Reaktion auf Informationssicherheitsvorfälle	M_042 Security Event Management (SIEM / SOD)	Ja	B, R
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen		Ja	B, R
A.5.28	Sammeln von Beweismaterial		Ja	G, B, R
A.5.29	Informationssicherheit bei Störungen		Ja	B, R
A.5.30	IKT-Bereitschaft für Business Continuity	M_073 Umsetzung A5.30 IKT-Bereitschaft für Business-Continuity	Ja	B, R
A.5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen		Ja	G, B, R
A.5.32	Geistige Eigentumsrechte	M_017 Maßnahmen zur Verbesserung der geistigen Eigentumsrechte verbessern	Ja	G, B, R
A.5.33	Schutz von Aufzeichnungen		Ja	G, B, R
A.5.34	Datenschutz und Schutz personenbezogener Daten (pbD)		Ja	G, B, R
A.5.35	Unabhängige Überprüfung der Informationssicherheit		Ja	G, B, R
A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit		Ja	B, R
A.5.37	Dokumentierte Betriebsabläufe		Ja	B, R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.6	**Personenbezogene Maßnahmen**		Ja	
A.6.1	Sicherheitsüberprüfung		Ja	B, R
A.6.2	Beschäftigungs- und Vertragsbedingungen		Ja	G, B, R
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	M_039 Etablierung regelmäßiger Awareness-Maßnahmen (Phishing-Simulation)	Ja	B, R
A.6.4	Maßregelungsprozess		Ja	B, R
A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung		Ja	B, R
A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen		Ja	V, R
A.6.7	Telearbeit	M_054 OFI #14 Prüfung der Dokumente bzgl. des sprachlichen Verbindlichkeitsgrads	Ja	G, B, R
A.6.8	Meldung von Informationssicherheitsereignissen		Ja	G, B, R
A.7	**Physische Maßnahmen**		Ja	
A.7.1	Physische Sicherheitsperimeter		Ja	V, R
A.7.2	Physischer Zutritt		Ja	V, R
A.7.3	Sichern von Büros, Räumen und Einrichtungen		Ja	R
A.7.4	Physische Sicherheitsüberwachung		Ja	B, R
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen		Ja	R
A.7.6	Arbeiten in Sicherheitsbereichen		Ja	R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren		Ja	B, R
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln		Ja	B, R
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten		Ja	R
A.7.10	Speichermedien		Ja	B, R
A.7.11	Versorgungseinrichtungen		Ja	B, R
A.7.12	Sicherheit der Verkabelung		Ja	B, R
A.7.13	Instandhaltung von Geräten und Betriebsmitteln		Ja	B, R
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln		Ja	R
A.8	**Technologische Maßnahmen**		Ja	
A.8.1	Endpunktgeräte des Benutzers	M_014 OFI #15 Überprüfung von BYOD-Risiko und -Maßnahmen, M_054 OFI #14 Prüfung der Dokumente bzgl. des sprachlichen Verbindlichkeitsgrads, M_060 Patch-Management für Betriebssysteme verbessern	Ja	B, R
A.8.2	Privilegierte Zugangsrechte		Ja	B, R
A.8.3	Informationszugangsbeschränkung		Ja	B, R
A.8.4	Zugriff auf den Quellcode		Ja	R
A.8.5	Sichere Authentifizierung		Ja	V, B, R
A.8.6	Kapazitätssteuerung		Ja	B, R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.8.7	Schutz gegen Schadsoftware	M_043 Einrichten von Virenschutzsoftware auf Clients und Servern	Ja	V, B, R
A.8.8	Handhabung von technischen Schwachstellen		Ja	B, R
A.8.9	Konfigurationsmanagement	K_016 Konfigurationsmanagement - Prüfung Firewall, K_017 Konfigurationsmanagement - Prüfung ThreatDown / Malwarebytes, K_020 Konfigurationsmanagement - Object Sync	Ja	B, R
A.8.10	Löschung von Informationen	M_019 Erstellung eines Löschkonzepts	Ja	B, R
A.8.11	Datenmaskierung	M_020 Konzept zur Datenmaskierung	Ja	R
A.8.12	Verhinderung von Datenlecks	M_021 Verhinderung von Datenlecks	Ja	B, R
A.8.13	Sicherung von Information	K_005 Sicherung von Information (Wiederherstellungstests von Backups)	Ja	B, R
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen		Ja	B, R
A.8.15	Protokollierung	K_013 Ereignisprotokollierung	Ja	G, B, R
A.8.16	Überwachung von Aktivitäten		Ja	B, R
A.8.17	Uhrensynchronisation		Ja	B, R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten		Ja	R
A.8.19	Installation von Software auf Systemen im Betrieb		Ja	B, R
A.8.20	Netzwerksicherheit		Ja	R
A.8.21	Sicherheit von Netzwerkdiensten		Ja	R
A.8.22	Trennung von Netzwerken		Ja	R
A.8.23	Webfilterung		Ja	R
A.8.24	Verwendung von Kryptographie	M_023 Aktualisierung der Kryptographie-Richtlinie	Ja	B, R
A.8.25	Lebenszyklus einer sicheren Entwicklung	M_044 ABW #2 Abweichung Sichere SW Entwicklung in Projekten	Ja	R
A.8.26	Anforderungen an die Anwendungssicherheit	M_044 ABW #2 Abweichung Sichere SW Entwicklung in Projekten	Ja	B, R
A.8.27	Sichere Systemarchitektur und technische Grundsätze		Ja	B, R
A.8.28	Sicheres Coding	M_024 Coding Guidelines für Sprachen/Technologien erstellen	Ja	B, R
A.8.29	Sicherheitsprüfung in Entwicklung und Abnahme		Ja	B, R
A.8.30	Ausgegliederte Entwicklung		Ja	B, R
A.8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen		Ja	V, B, R
A.8.32	Änderungssteuerung		Ja	B, R
A.8.33	Prüfinformationen		Ja	B, R

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Anw.	Begründung
A.8.34	Schutz der Informationssysteme während der Überwachungsprüfung		Ja	B, R