VORLAGE FÜR EINE CHECKLISTE ZUR BEWERTUNG VON CYBERSICHERHEITSRISIKEN (BEISPIEL)

ISO 27001 CONTROL	IMPLEMENTIERUNGSPHASE	AUFGABEN	KONFORM?	ANMERKUNGEN
5	***Informationssicherheitsrichtlinien***			
5.1	**Managementausrichtung für Informationssicherheit**			
5.1.1	Richtlinien für die Informationssicherheit	Gibt es Sicherheitsrichtlinien?	☐	
		Alle Richtlinien wurden vom Management genehmigt?	☐	
		Nachweis für Compliance?	☐	
6	***Organisation der Informationssicherheit***			
6.1	**Rollen und Verantwortlichkeiten in der Informationssicherheit**			
6.1.1	Sicherheitsrollen und -verantwortlichkeiten	Rollen und Verantwortlichkeiten wurden definiert?	☐	
6.1.2	Trennung von Aufgaben	Trennung von Aufgaben definiert?	☐	
6.1.3	Kontakt mit Behörden	Verifizierungsstelle / Behörde zur Überprüfung der Compliance kontaktiert?	☐	
6.1.4	Kontakt mit Interessensgruppen	Haben Sie Kontakt zu speziellen Interessengruppen bezüglich Compliance hergestellt?	☐	
6.1.5	Informationssicherheit im Projektmanagement	Nachweis der Informationssicherheit im Projektmanagement?	☐	
6.2	**Mobilgeräte und Telearbeit**			
6.2.1	Richtlinie für Mobilgeräte	Richtlinie für Mobilgeräte definiert?	☐	
6.2.2	Telearbeit	Richtlinie für Remote-Arbeit festgelegt?	☐	
7	***Sicherheit im Personalwesen***			
7.1	**Vor der Anstellung**			
7.1.1	Screening	Richtlinie für die Überprüfung von Mitarbeitern vor der Anstellung definiert?	☐	
7.1.2	Beschäftigungsbedingungen	Richtlinie für HR-Bedingungen und -Beschäftigungsverhältnisse definiert?	☐	
7.2	**Während der Beschäftigung**			
7.2.1	Verantwortlichkeiten des Managements	Richtlinien für Verantwortlichkeiten des Managements definiert?	☐	
7.2.2	Informationssicherheit – Bewusstsein, Ausbildung und Training	Richtlinien für das Bewusstsein für Informationssicherheit, Bildung und Training definiert?	☐	
7.2.3	Disziplinarverfahren	Richtlinien für Disziplinarverfahren in Bezug auf die Informationssicherheit definiert?	☐	

7.3	**Kündigung und Wechsel des Beschäftigungsverhältnisses**			
7.3.1	Kündigung oder Änderung des Beschäftigungsverhältnisses	Richtlinien für die Beendigung oder den Wechsel des Arbeitsverhältnisses in Bezug auf die Informationssicherheit definiert?	☐	
8	***Asset-Management***			
8.1	**Zuständigkeiten für Assets**			
8.1.1	Bestand an Assets	Vollständige Bestandsliste der Assets?	☐	
8.1.2	Eigentum an Assets	Vollständige Eigentümerliste für Assets	☐	
8.1.3	Zulässige Nutzung von Assets	Richtlinie zur „zulässigen Nutzung“ von Assets definiert?	☐	
8.1.4	Rückgabe von Assets	Richtlinie für die Rückgabe von Assets definiert?	☐	
8.2	**Informationsklassifizierung**			
8.2.1	Informationsklassifizierung	Richtlinie zur Klassifizierung von Informationen definiert?	☐	
8.2.2	Kennzeichnung von Informationen	Richtlinie für die Kennzeichnung von Informationen definiert?	☐	
8.2.3	Umgang mit Assets	Richtlinie für den Umgang mit Assets definiert?	☐	
8.3	**Umgang mit Medien**			
8.3.1	Management von Datenträgern	Richtlinie für den Umgang mit Datenträgern definiert?	☐	
8.3.2	Entsorgung von Medien	Richtlinie für die Entsorgung von Medien definiert?	☐	
8.3.3.	Übertragung physischer Medien	Richtlinie für die Übertragung physischer Medien definiert?	☐	
9	***Zugriffssteuerung***			
9.1	**Zuständigkeiten für Assets**			
9.1.1	Richtlinie für die Zugriffskontrolle	Richtlinie für die Zugriffskontrolle definiert?	☐	
9.1.2	Zugriff auf Netzwerke und Netzwerkdienste	Richtlinie für den Zugriff auf Netzwerke und Netzwerkdienste definiert?	☐	
9.2	**Zuständigkeiten für Assets**			
9.2.1	Benutzerregistrierung und -abmeldung	Richtlinie für die An- und Abmeldung von Benutzer-Assets definiert?	☐	
9.2.2	Bereitstellung des Benutzerzugriffs	Richtlinie für die Bereitstellung des Benutzerzugriffs definiert?	☐	
9.2.3	Verwaltung privilegierter Zugriffsrechte	Richtlinie für die Verwaltung privilegierter Zugriffsrechte definiert?	☐	

9.2.4	Verwaltung von geheimen Authentifizierungsinformationen der Benutzer	Richtlinie für die Verwaltung von geheimen Authentifizierungsinformationen der Benutzer definiert?	☐	
9.2.5	Überprüfung der Benutzerzugriffsrechte	Richtlinie zur Überprüfung der Benutzerzugriffsrechte definiert?	☐	
9.2.6	Entfernung oder Anpassung von Zugriffsrechten	Richtlinie für die Entfernung oder Anpassung von Zugriffsrechten definiert?	☐	
9.3	**Benutzerverantwortlichkeiten**			
9.3.1	Nutzung von geheimen Authentifizierungsinformationen	Richtlinie zur Nutzung von geheimen Authentifizierungsinformationen definiert?	☐	
9.4	**System- und Anwendungszugriffskontrolle**			
9.4.1	Beschränkung des Zugriffs auf Informationen	Richtlinie zur Beschränkung des Zugriffs auf Informationen definiert?	☐	
9.4.2	Sichere Anmeldeverfahren	Richtlinie für sichere Anmeldeverfahren definiert?	☐	
9.4.3	Kennwortmanagementsystem	Richtlinie für Kennwortmanagementsysteme definiert?	☐	
9.4.4	Verwendung von privilegierten Dienstprogrammen	Richtlinie für die Verwendung von privilegierten Dienstprogrammen definiert?	☐	
9.4.5	Steuerung des Zugriffs auf Programmquellcode	Richtlinie für die Steuerung des Zugriffs auf Programmquellcode definiert?	☐	
10	***Kryptografie***			
10.1	**Kryptografische Steuerung**			
10.1.1	Richtlinie zur Verwendung kryptographischer Steuerungen	Richtlinie zur Verwendung kryptografischer Steuerungen definiert?	☐	
10.1.2	Schlüsselmanagement	Richtlinien für das Schlüsselmanagement definiert?	☐	
11	***Physische und Umgebungssicherheit***			
11.1	**Sichere Bereiche**			
11.1.1	Physischer Sicherheitsbereich	Richtlinien für physische Sicherheitsbereiche definiert?	☐	
11.1.2	Physische Zutrittskontrollen	Richtlinie für physische Zugangskontrollen definiert?	☐	
11.1.3	Absicherung von Büros, Räumen und Anlagen	Richtlinien für die Absicherung von Büros, Räumen und Anlagen definiert?	☐	
11.1.4	Schutz gegen externe und Umweltbedrohungen	Richtlinien zum Schutz gegen externe und Umweltbedrohungen definiert?	☐	
11.1.5	Arbeiten in sicheren Bereichen	Richtlinie für die Arbeit in sicheren Bereichen definiert?	☐	
11.1.6	Liefer- und Ladebereiche	Richtlinien für Liefer- und Ladebereiche definiert?	☐	

11.2	**Ausrüstung**			
11.2.1	Standortwahl und Schutz der Ausrüstung	Richtlinien für die Standortwahl und Schutz der Ausrüstung definiert?	☐	
11.2.2	Hilfsversorgungseinrichtungen	Richtlinie für Hilfsversorgungseinrichtungen definiert?	☐	
11.2.3	Verkabelungssicherheit	Richtlinie für die Verkabelungssicherheit definiert?	☐	
11.2.4	Gerätewartung	Richtlinie für die Gerätewartung definiert?	☐	
11.2.5	Entfernen von Assets	Richtlinie für das Entfernen von Assets definiert?	☐	
11.2.6	Sicherheit von Ausrüstung und Assets, die nicht vor Ort sind	Richtlinie für die Sicherheit von Ausrüstung und Assets definiert, die nicht vor Ort sind?	☐	
11.2.7	Sichere Entsorgung oder Wiederverwendung von Ausrüstung	Sichere Entsorgung oder Wiederverwendung von Ausrüstung?	☐	
11.2.8	Unbeaufsichtigte Benutzerausrüstung	Richtlinie für unbeaufsichtigte Benutzerausrüstung definiert?	☐	
11.2.9	Clear Desk- und Clear-Screen-Richtlinien	Richtlinie für Clear Desk- und Clear-Screen-Richtlinien definiert?	☐	
12	***Betriebssicherheit***			
12.1	**Betriebliche Verfahren und Aufgaben**			
12.1.1	Dokumentierte Betriebsabläufe	Richtlinie für dokumentierte Betriebsabläufe definiert?	☐	
12.1.2	Change-Management	Richtlinien für das Changemanagement definiert?	☐	
12.1.3	Kapazitätsmanagement	Richtlinien für das Kapazitätsmanagement definiert?	☐	
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	Richtlinien für die Trennung von Entwicklungs-, Test- und Betriebsumgebungen definiert?	☐	
12.2	**Schutz vor Malware**			
12.2.1	Malware-Kontrollen	Richtlinien für Malware-Kontrolle definiert?	☐	
12.3	**System-Backup**			
12.3.1	Back-up	Richtlinie für die Sicherung von Systemen definiert?	☐	
12.3.2	Back-up von Informationen	Richtlinie für die Sicherung von Informationen definiert?	☐	
12.4	**Protokollierung und Überwachung**			
12.4.1	Protokollierung von Ereignissen	Richtlinie für die Ereignisprotokollierung definiert?	☐	

12.4.2	Schutz von Protokollinformationen	Richtlinie zum Schutz von Protokollinformationen definiert?	☐	
12.4.3	Administratoren- und Bedienerprotokoll	Richtlinie für Administratoren- und Bedienerprotokoll definiert?	☐	
12.4.4	Uhrsynchronisierung	Richtlinie für die Uhrsynchronisierung definiert?	☐	
12.5	**Steuerung der betrieblichen Software**			
12.5.1	Installation von Software in betrieblichen Systemen	Richtlinie für die Installation von Software in betrieblichen Systemen definiert?	☐	
12.6	**Technisches Schwachstellenmanagement**			
12.6.1	Verwaltung technischer Anfälligkeiten	Richtlinie für die Verwaltung technischer Schwachstellen definiert?	☐	
12.6.2	Einschränkung von Softwareinstallationen	Richtlinie für die Einschränkung von Softwareinstallationen definiert?	☐	
12.7	**Überlegungen zur Prüfung von Informationssystemen**			
12.7.1	Kontrolle von Informationssystem-Audits	Richtlinie für die Kontrolle von Informationssystem-Audits definiert?	☐	
13	***Kommunikationssicherheit***			
13.1	**Netzwerksicherheitsmanagement**			
13.1.1	Netzwerkkontrollen	Richtlinie für Netzwerksteuerung definiert?	☐	
13.1.2	Sicherheit von Netzwerkdiensten	Richtlinie für die Sicherheit von Netzwerkdiensten definiert?	☐	
13.1.3	Trennung von Netzwerken	Richtlinie für die Trennung von Netzwerken definiert?	☐	
13.2	**Informationsübertragung**			
13.2.1	Richtlinien und Vorgehensweisen bei Informationsübertragungen	Richtlinie für Richtlinien und Vorgehensweisen bei Informationsübertragungen definiert?	☐	
13.2.2	Vereinbarungen zur Informationsübertragung	Richtlinien für Vereinbarungen zur Informationsübertragung definiert?	☐	
13.2.3	Elektronische Nachrichtenübermittlung	Richtlinie für elektronische Nachrichtenübermittlung definiert?	☐	
13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Richtlinie für Vertraulichkeits- oder Geheimhaltungsvereinbarungen definiert?	☐	
13.2.5	Systemakquise, -entwicklung und -wartung	Richtlinie für Systemakquise, -entwicklung und -wartung definiert?	☐	
14	***Systemakquise, -entwicklung und -wartung***			
14.1	**Sicherheitsanforderungen an Informationssysteme**			
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	Richtlinie für die Analyse und Spezifikation von Informationssicherheitsanforderungen definiert?	☐	

14.1.2	Absicherung von Anwendungsdiensten in öffentlichen Netzwerken	Richtlinie zur Absicherung von Anwendungsdiensten in öffentlichen Netzwerken definiert?	☐	
14.1.3	Schutz von Transaktionen in Anwendungsdiensten	Richtlinie zum Schutz von Transaktionen in Anwendungsdiensten definiert?	☐	
14.2	**Sicherheit in Entwicklungs- und Unterstützungsprozessen**			
14.2.1	Interne Entwicklung	Richtlinie für die interne Entwicklung definiert?	☐	
15	***Lieferantenbeziehungen***			
15.1.1	Lieferantenbeziehungen	Richtlinie für Lieferantenbeziehungen definiert?	☐	
16	***Management von Informationssicherheitsvorfällen***			
16.1.1	Management der Informationssicherheit	Richtlinien für das Informationssicherheitsmanagement definiert?	☐	
17	***Informationssicherheitsaspekte des Geschäftskontinuitätsmanagements***			
17.1	**Kontinuität der Informationssicherheit**			
17.1.1	Kontinuität der Informationssicherheit	Richtlinien für die Informationssicherheitskontinuität definiert?	☐	
17.2	**Redundanzen**			
17.2.1	Redundanzen	Richtlinie für Redundanzen definiert?	☐	
18	***Compliance***			
18.1	**Compliance mit gesetzlichen und vertraglichen Anforderungen**			
18.1.1	Ermittlung geltender Rechtsvorschriften und vertraglicher Anforderungen	Richtlinie für die Ermittlung geltender Rechtsvorschriften und vertraglicher Anforderungen definiert?	☐	
18.1.2	Rechte an geistigem Eigentum	Richtlinien für Rechte an geistigem Eigentum definiert?	☐	
18.1.3	Schutz von Datensätzen	Richtlinie zum Schutz von Datensätzen definiert?	☐	
18.1.4	Datenschutz und Schutz personenbezogener Daten	Richtlinie für den Datenschutz und Schutz personenbezogener Daten definiert?	☐	
18.1.5	Regulierung kryptografischer Steuerung	Richtlinie zur Regulierung kryptografischer Steuerung definiert?	☐	
18.1	**Unabhängige Überprüfung der Informationssicherheit**			
18.1.1	Einhaltung von Sicherheitsrichtlinien und -standards	Richtlinie zur Einhaltung von Sicherheitsrichtlinien und -standards definiert?	☐	
18.1.2	Prüfung technischer Compliance	Richtlinie für die Prüfung technischer Compliance definiert?	☐	

HAFTUNGSAUSSCHLUSS

Alle von Smartsheet auf der Website aufgeführten Artikel, Vorlagen oder Informationen dienen lediglich als Referenz. Wir versuchen, die Informationen stets zu aktualisieren und zu korrigieren. Wir geben jedoch, weder ausdrücklich noch stillschweigend, keine Zusicherungen oder Garantien jeglicher Art über die Vollständigkeit, Genauigkeit, Zuverlässigkeit, Eignung oder Verfügbarkeit in Bezug auf die Website oder die auf der Website enthaltenen Informationen, Artikel, Vorlagen oder zugehörigen Grafiken. Die Nutzung dieser Informationen erfolgt deshalb auf eigenes Risiko.

Diese Vorlage wird nur als Beispiel bereitgestellt. Diese Vorlage ist in keiner Form als rechtliche oder Compliance-Beratung gedacht. Benutzer dieser Vorlage müssen feststellen, welche Informationen notwendig und erforderlich sind, um ihre Ziele zu erreichen.