Checkliste für Pflichtdokumente aus ISO/IEC 27001:2013

Bitte füllen Sie den nachfolgenden Fragebogen zur Implementierung der ISO/IEC 27001:2013 aus.

Auf Basis Ihrer Antworten werden wir uns detailliert mit Ihnen in einem persönlichen Gespräch austauschen und ein für Ihr Unternehmen passendes Angebot zur Implementierung der ISO 27001 erstellen.

	Erforderliche Pflichtdokumente	**Abschnitte gemäß ISO 27001:2013**	**Vorhanden?**	**Wenn „ja" – Ablageort Wenn „nein" – warum nicht?**
1.	Ist der **Anwendungsbereich des ISMS** definiert und dokumentiert?	4.3		
2.	Ist die **Leitlinie zur Informationssicherheit** abgestimmt und dokumentiert?	5.2		
3.	Ist die **Risikobewertungs- und Risikobehandlungsmethodik** definiert?	6.1.2		
4.	Ist eine **Anwendbarkeitserklärung** (mit den notwendigen Maßnahmen) vorhanden?	6.1.3 d)		
5.	Ist ein **Risikobehandlungsplan** formuliert und dokumentiert? Sie die **Ergebnisse der Risikobehandlung** dokumentiert?	6.1.3 e) und 8.3		
6.	Sind die **Informationssicherheitsziele** festgelegt und dokumentiert?	6.2		
7.	Sind **die Aufzeichnungen über Schulungen, Fähigkeiten, Erfahrung und Qualifikationen** der Mitarbeiter vorhanden?	7.2		
8.	Ist ein **Risikobewertungsbericht** vorhanden?	8.2		
9.	Wurden die **Überwachungs- und Messergebnisse** ausgewertet?	9.1		
10.	Ist ein **internes Audit-Programm** vorhanden?	9.2		
11.	Sind die **Ergebnisse interner Audits** vorhanden ausgewertet?	9.2		
12.	Sind die **Ergebnisse aus Managementbewertungen** vorhanden?	9.3		
13.	Sind die **Ergebnisse von Korrekturmaßnahmen** vorhanden?	10.1		
14.	Sind die **Sicherheits-Rollen und Verantwortlichkeiten** definiert?	A.7.2.1		

	Erforderliche Pflichtdokumente	Abschnitte gemäß ISO 27001:2013	Vorhanden?	Wenn „ja“ – Ablageort Wenn „nein“ – warum nicht?
15.	Ist ein **Verzeichnis der Informationen** vorhanden?	A.8.1.1		
16.	Sind Regeln zum **Umgang mit Informationen** definiert?	A.8.1.3		
17.	Ist eine **Richtlinie für die Zugriffskontrolle** dokumentiert und kommuniziert?	A.9.1.1		
18.	Ist die **Richtlinie für die Verwendung von kryptographischen Algorithmen** vorhanden?	A 10.1.1		
19.	Sind **Betriebsprozesse** dokumentiert und werden diese allen Nutzern zur Verfügung gestellt?	A.12.1.1		
20.	Werden **Logdateien** erstellt, aufbewahrt und regelmäßig ausgewertet?	A.12.4.1 und A.12.4.3		
21.	Sind Anforderungen zur Einhaltung der **Vertraulichkeit und Geheimhaltung mit Kunden und Lieferanten** vereinbart?	A.13.2.4		
22.	Sind **Prinzipien zum sicheren Betrieb der Systeme** festgelegt?	A.14.2.5		
23.	Gibt es eine Richtlinie für **Lieferantenbeziehungen** und wurde diese kommuniziert?	A.15.1.1		
24.	Ist ein Verfahren zum **Umgang mit Sicherheitsvorfällen** definiert und kommuniziert?	A.16.1.5		
25.	Ist die **Informationssicherheit** ein wesentlicher Bestandteil des BCM?	A.17.1.2		
26.	Sind alle **gesetzlichen, behördlichen und vertraglichen Anforderungen erfasst** und erfüllt?	A.18.1.1		

➔ Eine ausführliche Studie zum Thema ***„Why should you trust ISO 27001?“*** finden Sie auf unserer Webseite https://alps-gmbh.de/studie-zum-thema-why-should-you-trust-iso-27001/

Haben Sie Fragen? - Wir helfen Ihnen gerne weiter und freuen uns gemeinsam mit Ihnen auf die Umsetzung!

Ihr ALPS-Experten-Team