Checkliste zur TISAX® Umsetzung

basierend auf VDA-ISA Information Security Assessment

Bitte füllen Sie den nachfolgenden Fragebogen aus - auf Basis Ihrer Antworten werden wir uns in einem persönlichen Gespräch detailliert mit Ihnen austauschen und ein für Ihr Unternehmen passendes Angebot zur TISAX® Umsetzung erstellen.

	Erforderliche Pflichtdokumente	Abschnitte gemäß VDA-ISA	Vorhanden?	Wenn „ja“ – Ablageort Wenn „nein“ – warum nicht?
1.	Ist der **Anwendungsbereich des ISMS** definiert und dokumentiert?	1.1		
2.	Ist die **Leitlinie zur Informationssicherheit** abgestimmt und dokumentiert?	1.1		
3.	Ist die **Risikobewertungs- und Risikobehandlungsmethodik** definiert?	1.2		
4.	Ist eine **Selbsteinschätzung** gemäß VDA-ISA vorhanden?	6.1.3 d)		
5.	Ist ein **Risikobehandlungsplan** formuliert und dokumentiert? Sind die **Ergebnisse der Risikobehandlung** dokumentiert?	1.2		
6.	Sind die **Informationssicherheitsziele** festgelegt und dokumentiert?	1.1		
7.	Sind **die Aufzeichnungen über Schulungen, Fähigkeiten, Erfahrung und Qualifikationen** der Mitarbeiter vorhanden?	7.2		
8.	Ist ein **Risikobewertungsbericht** vorhanden?	1.2		
9.	Wurden die **Überwachungs- und Messergebnisse** ausgewertet?	1.3		
10.	Sind die **Ergebnisse aus Managementbewertungen** vorhanden?	1.3		
11.	Sind die **Ergebnisse von Korrekturmaßnahmen** vorhanden?	10.1		
12.	Sind die **Sicherheits-Rollen und Verantwortlichkeiten** definiert?	6.1		
13.	Ist ein **Verzeichnis der Informationen** vorhanden?	8.1		
14.	Sind Regeln zum **Umgang mit Informationen** definiert?	8.1		

	Erforderliche Pflichtdokumente	Abschnitte gemäß VDA-ISA	Vorhanden?	Wenn „ja“ – Ablageort Wenn „nein“ – warum nicht?
15.	Ist eine **Richtlinie für die Zugriffskontrolle** dokumentiert und kommuniziert?	9.1		
16.	Ist die **Richtlinie für die Verwendung von kryptographischen Algorithmen** vorhanden?	10.1		
17.	Werden **Logdateien** erstellt, aufbewahrt und regelmäßig ausgewertet?	12.5		
18.	Sind Anforderungen zur Einhaltung der **Vertraulichkeit und Geheimhaltung mit Kunden und Lieferanten** vereinbart?	13.5		
19.	Sind **Prinzipien zum sicheren Betrieb der Systeme** festgelegt?	14.2		
20.	Gibt es eine Richtlinie für **Lieferantenbeziehungen** und wurde diese kommuniziert?	15.1		
21.	Ist ein Verfahren zum **Umgang mit Sicherheitsvorfällen** definiert und kommuniziert?	16.1		
22.	Ist die **Informationssicherheit** ein wesentlicher Bestandteil des BCM?	17.1		
23.	Sind alle **gesetzlichen, behördlichen und vertraglichen Anforderungen erfasst** und erfüllt?	18.1		

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

Ihr com3+ GmbH-Experten-Team