



# **ANHANG 17-G**

## **ZERTIFIZIERUNGSANFORDERUNGEN CHECKLISTE**

November 2024

Dieses Dokument enthält firmeneigene Informationen der MAN Truck & Bus.  
Dieses Dokument und die darin enthaltenen Informationen dürfen nur mit  
ausdrücklicher vorheriger schriftlicher Zustimmung der MAN Truck & Bus  
veröffentlicht, weitergegeben oder zu anderen Zwecken eingesetzt werden.

## INHALT

<b>EINLEITUNG (KONFORMITÄTSANFORDERUNGEN AN DIE MANAGEMENTPRAKTIKEN DES AUFTRAGNEHMERS).....</b>	<b>3</b>
<b>1.0 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) (ISO/IEC 27001).....</b>	<b>3</b>
<b>2.0 TISAX (VDA-ISA) .....</b>	<b>3</b>
<b>3.0 CLOUD .....</b>	<b>4</b>

EINLEITUNG (KONFORMITÄTSANFORDERUNGEN AN DIE MANAGEMENTPRAKTIKEN DES AUFTRAGNEHMERS)			
<p>Das MAN Truck &amp; Bus Informationssicherheitsmanagementsystem (ISMS) basiert auf dem Standard ISO/IEC 27001 und entspricht den Anforderungen des VDA ISA (TISAX).</p> <p>Der Auftragnehmer muss Informationen über den Stand und die Umsetzung der geltenden Zertifizierungen im Zusammenhang mit der Erbringung der Dienstleistung für MAN Truck &amp; Bus vorlegen.</p> <p>Mit dieser Checkliste soll sichergestellt werden, dass der Auftragnehmer die geeigneten Maßnahmen ergriffen hat und damit allen Bedrohungen begegnet, die sich aus dem Zugang zu, der Verarbeitung und/oder der Speicherung von Informationen im Rahmen der Dienstleistungserbringung ergeben. Damit wird auch die kontinuierliche Verbesserung und weitere Sorgfaltspflicht des Informationssicherheitsmanagementsystems des Auftragnehmers und seiner Unterauftragnehmer bescheinigt.</p>			
Ref #	Nachweis grundlegender Informationssicherheitszertifizierungen	Ja/Nein	Kommentar
1.0 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) (ISO/IEC 27001)			
Anl. 17-G – 1.	Der Auftragnehmer hat ein zertifiziertes Managementsystem für die Informationssicherheit nach ISO/IEC 27001 eingeführt, das alle Einheiten und jeweiligen Standorte umfasst, die mit der Erbringung der Dienstleistung in Zusammenhang stehen.		
Anl. 17-G – 2.	Der Auftragnehmer hat auch die folgenden Erweiterungen des Geltungsbereichs seiner ISO/IEC 27001-Zertifizierungen erreicht: - ISO 27017 in Bezug auf die Bereitstellung und Nutzung von Cloud-Diensten - ISO 27018 in Bezug auf den Schutz personenbezogener Daten (PII) in der Cloud		
Anl. 17-G – 3.	Der Auftragnehmer plant, die folgenden Zertifizierungen innerhalb der nächsten 9 bis 12 Monate zu erlangen: - ISO/IEC 27001 - Erweiterung der ISO/IEC 27001 (bitte kommentieren)		
2.0 TISAX (VDA-ISA)			
Anl. 17-G – 4.	Der Auftragnehmer kann eine gültige TISAX-Bewertung mit relevantem Umfang (Label) für alle Einheiten, die mit der Leistungserbringung zusammenhängen, zur Verfügung stellen. Bitte geben Sie die Informationen über die ENX-		

	Datenbank an die VW-Teilnehmer-ID "PVPT9Z" weiter.		
Anl. 17-G – 5.	Der Auftragnehmer plant, diese Zertifizierung innerhalb der nächsten 9 bis 12 Monate zu erreichen.		
<b>Ref #</b>	<b>Nachweis weiterer Zertifizierungen (zusätzlich zu den oben genannten) - bitte geben Sie die Bewertungsstufe in den Kommentaren an</b>	<b>Ja/Nein</b>	<b>Kommentar</b>
<b>3.0 CLOUD</b>			
Anl. 17-G – 6.	Third Party Cloud Assessment		
Anl. 17-G – 7.	BSI C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI))		
Anl. 17-G – 8.	CSA STAR (Cloud Security Alliance)		
Anl. 17-G – 9.	Der Auftragnehmer plant, eine der oben genannten Cloud-Zertifizierungen innerhalb der nächsten 9-12 Monate zu erlangen - bitte geben Sie in den Kommentaren an, welche.		