Fragebogen

• Betreibt das Unternehmen ein Informationssicherheits-Management-System (ISMS)?

_____

• Betreibt das Unternehmen ein Cyber Security Management System (CSMS)?

_____

• Betreibt das Unternehmen ein Software Update Management System (SUMS)?

_____

• Bestehen für diese(s) System(e) eine Zertifizierung, zum Beispiel nach ISO 21434 oder eine Prüfung nach den Anforderungen des Kraftfahrtbundesamtes (KBA)?

_____

• Existiert im Unternehmen ein benannter Cyber Security Manager?

_____

• Gibt es im Unternehmen eine Cyber Security Management Richtlinie?

_____

• Wie werden die Mitarbeiter über die Gefahren beim Umgang mit cyber-security relevanten Informationen und deren Verarbeitung informiert? (Schulungen, Informationstage o.ä.)

_____

• Werden Mitarbeiter geschult und sensibilisiert? (hinsichtlich Cyber Security)

_____

• Wurde eine TARA (Threat and Risk Analysis) für die Produkte/Komponenten durchgeführt nach ISO 21434 und werden die erkannten Risiken entsprechend behandelt?

_____

• Wird vor Auftragsvergabe an Fremdfirmen die Cyber Security der Auftragnehmer geprüft und sichergestellt?

_____

• Wie wird die Geheimhaltung bei der Zusammenarbeit mit Fremdfirmen sichergestellt?

_____

• Werden interne Audits zur Überprüfung der Cyber Security durchgeführt?

_____

• Existiert eine Zutrittssteuerung in Ihrem Unternehmen?

_____

• Existiert eine Sicherheitszonenkonzept in Ihrem Unternehmen und wenn ja, wie ist dieses Aufgebaut?

_____

• Wie ist das Unternehmen gegen umgebungsbezogene Bedrohungen geschützt?

_____

• Wie werden Backups erstellt und die erfolgreiche Durchführung kontrolliert?

_____

• Werden regelmäßige Restore-Tests durchgeführt? (Wiederherstellung der Backups)

_____

• Wie werden Back-End-Server geschützt?

_____

• Gibt es segmentierte Netzwerke im Unternehmen? (z.B. Gästenetzwerk und Produktivnetzwerk)

_____

• Gibt es ein Konzept wie Software-Stände und Software-Update der E/E-Produkte über den Produkt-Lebenszyklus gemanaged werden?

_____

• Wie wird der Zugriff durch Dritte auf das Unternehmensnetz geregelt (z.B. Dienstleister)?

_____

• Gibt es Richtlinien im Unternehmen für den Umgang mit mobilen Datenträgern?

_____

• Gibt es im Unternehmen einen Prozess zur sicheren Entsorgung von Datenträgern?

_____

• Gibt es eine Leitlinie zur Anwendung von Verschlüsselung und kryptografischen Maßnahmen?

_____

• Inwiefern sind Maßnahmen für das Cyber Security Monitoring und das Schwachstellenmanagement etabliert?

_____

• Inwieweit ist das Arbeiten mit mobilen Geräten geregelt?

_____

• Gibt es eine Anordnung zur Einhaltung der Ordnung? (z.B. clean desk policy)

_____

• Existiert eine Richtlinie zum Patch-Management?

_____

• Wie werden Unternehmensnetzwerke vor Schadsoftware geschützt?

_____

• Werden Informationen im Unternehmen klassifiziert? (z.B. öffentlich, intern, vertraulich & streng vertraulich)

_____

• Gibt es Definitionen zum Umgang mit Informationen entsprechend einer Klassifizierung? (z.B. Handhabung, Transport, Speicherung und Löschung)

_____

• Gibt es Sicherheitseinrichtungen für Notfälle? (z.B. Brandschutzzonen, redundante Systeme o.ä.)