Angaben zum Hersteller[1]

Registriernummer:

Name:

Auditierter Standort:

Auditdatum:

Auditor(in):

Allgemeines

Dieser Anforderungskatalog enthält die Forderungen der UN-R 155/156 und des Typgenehmigungsverfahrens des Kraftfahrt-Bundesamtes in Bezug auf ein Cybersecurity- und/oder Softwareupdate-Managementsystem. Er bildet

- nach Selbstauskunft durch den Hersteller: die Grundlage für die Auditplanung
- nach Ergänzung durch die Auditoren: als Bestandteil des Auditberichts die Grundlage für die Entscheidung des KBA über die Ausstellung eines Zertifikats entsprechend UN-R 155 und 156 Abschnitt 6.

Die Anforderungen gelten für alle Standorte, Prozesse und Produkte/Dienstleistungen[2], die in das Zertifikat eingeschlossen sind.

Grundsätzlich muss ein Hersteller alle Anforderungen erfüllen. Sofern einzelne Anforderungen nicht anwendbar sind, kann der Hersteller dies mit einer Begründung entsprechend eintragen. Der Auditor/die Auditorin ist nicht an diese Aussage des Herstellers gebunden, wird sie aber in der Auditvorbereitung berücksichtigen.

Ziel des Audits ist es nicht, 100% Sicherheit nachzuweisen, sondern auf der Grundlage dokumentierter Anforderungen und objektiver Nachweise des Herstellers zu bestätigen, dass

- kein erhebliches Risiko für Sicherheit, Umwelt und Gesundheit im Rahmen des Scopes der UN-R 155/156 besteht
- die Forderungen der UN-Regelungen erfüllt werden können
- der Hersteller die von ihm dokumentierten Maßnahmen zufriedenstellend umgesetzt hat
- das Personal sich seiner Verantwortung zur Erfüllung der Anforderungen bewusst ist.

Hinweise zur Handhabung

Sofern sich Anforderungen auf Produktprüfungen (durch den Hersteller) beziehen, gelten die relevanten Anforderungen des Abschnittes 7.3 der UN-R 155 bzw. 7.2 der UN-R 156 mit (vgl. Angabe in Klammern).

Die Verwendung der Einzahl in den Anforderungen (z. B. ein Prozess) schließt nicht aus, dass die Umsetzung anders (z. B. in mehreren Prozessen) erfolgt.

---

[1] Der Begriff Hersteller wird hier als Synonym für „auditierte Organisation“ und derzeitiger bzw. künftiger Genehmigungsinhaber verwendet.

[2] Im Folgenden als Produkte bezeichnet.

Die Erfüllung einzelner Anforderungen ist ggf. in mehreren Auditphasen zu bewerten. Es wird erwartet, dass die Erfüllung der Anforderungen durch dokumentierte angemessene und wirksame Prozesse gewährleistet wird und diese Prozesse regelmäßig auf der Grundlage objektiver Kriterien und Nachweise bewertet werden.

Für Feststellungen werden folgende Kürzel verwendet:

- iO - ohne Mängel
- P - hervorzuhebende, positive Feststellung
- V - grundsätzlich in Ordnung, Verbesserungspotenzial vorhanden
- N - Nebenabweichung (mit Nummer des Feststellungsprotokolls)
- H - Hauptabweichung (mit Nummer des Feststellungsprotokolls)
- nb - nicht bewertet
- nz - nicht zutreffend (Begründung erforderlich, sofern nicht aus anderen Angaben ersichtlich)

Die Feststellungen P, V, N und H werden im Auditbericht in einer zusammenfassenden Tabelle im Abschnitt „Audit-Ergebnisse“ erläutert. Zusätzliche Erläuterungen zur Selbstauskunft trägt der Auditor/die Auditorin kursiv in die Spalte „Selbstauskunft und Prüfvermerke“ ein.

Für die vollständige Bewertung ist der Leitende Auditor/die Leitende Auditorin (diejenige Person, die den Auditbericht unterschreibt) verantwortlich. Führen mehrere Auditoren/Auditorinnen das Audit durch, kann der Anforderungskatalog entsprechend aufgeteilt werden. Es ist dabei sicherzustellen, dass nach Durchführung der Begutachtung ein komplett ausgefülltes Exemplar beim KBA vorliegt.

Der Anforderungskatalog umfasst
- Teil A: Allgemeine Anforderungen an Managementsysteme
- Teil B: Spezielle Anforderungen an CSMS/SUMS

Der Hersteller muss sicherstellen, dass die allgemeinen Anforderungen (Teil A) bei der Umsetzung der CSMS/SUMS-spezifischen Anforderungen zur Anwendung kommen, sofern dies angemessen ist. Die Referenzierung von Teil A in Teil B gibt dazu einen Anhaltspunkt, ist aber nicht abschließend und nicht in jedem Fall anwendbar.

Teil B verweist auf zu beachtende Anforderungen aus Teil A. Insofern ist Teil A nicht gesondert zu auditieren.

Abkürzungsverzeichnis

A	Aufzeichnung erforderlich [3]
B	Bewertung
CS	Cybersecurity
D	Dokumentierte Prozessbeschreibung o.ä. erforderlich
KBA	Kraftfahrt-Bundesamt
MS	Managementsystem
SU	Software-Update
TD	Technischer Dienst

Mitgeltende Dokumente

Auditbericht
Checkliste Risikobewertung
x Checklisten Prüfverfahren
x Checklisten Prozessprüfung

[3] Nachweise können oft nur bei Überwachungen/Re-Zertifizierungen eingesehen werden.

Teil A – Allgemeine Anforderungen an Managementsysteme

Lfd. Nr.	Ergänzende Anforderung	B
1	Führung nimmt ihre Verantwortung war	
2	Die Elemente, Prozesse, Anforderungen usw. des CSMS/SUMS stehen nicht in Widerspruch zu anderen Prozessen, Systemen, Vorgaben … der Organisation; die Nahtstellen sind ausreichend definiert	
3	Entscheidungen/Freigaben werden nach Möglichkeit unter Mitwirkung weitgehend neutraler Personen bzw. Gremien getroffen	
4	Ziele sind kaskadiert, konsistent, angemessen und messbar; Sie sind angemessen kommuniziert und werden regelmäßig aktualisiert	
5	Anforderungen - aus Zielen und Risikoanalyse abgeleitet - Angemessen - Dokumentiert (bei Notwendigkeit) - Erfüllung überwacht	
6	Prozess - Verantwortlichkeit/Befugnisse - Eingang/Verfahren/Ausgang/Nahtstelle zu anderen Prozessen - Leistungsindikatoren/Eignungskriterien (in Übereinstimmung mit Zielen) - Freigabe - Kompetenz - Arbeits-/Prüfmittel - Infrastruktur, Prozessumgebung, zeitliche Ressourcen usw. - Steuerung nichtkonformer Ergebnisse - Überwachung (angemessen, geeignet; Aufzeichnungen; Analyse) - Dokumentation	
7	Sonstige Feststellung der Konformität - Organisiert - Kompetent - Geeignet - aufgezeichnet	
8	Kennzeichnung und Rückverfolgbarkeit	
9	Wissen der Organisation (Informationsmanagement) - sinnvoll gesammelt, aufgezeichnet, gelenkt, analysiert, genutzt; - Angemessene Kommunikation - Schutz vor Verlust, Verfälschung, unberechtigtem Zugriff, Vertuschung, Verzögerung usw.	
10	Notwendige Kompetenz von Leitung, Ausführenden, Überwachenden (Wissen, Fähigkeiten, Fertigkeiten) des Personals - Festgelegt - Vorhanden - Art der Überprüfung und Kriterien festgelegt (erstmalig und wiederholt) - Aufzeichnungen zu den Kompetenzfeststellungen	
11	Alle relevanten Personen sind sich ihres Beitrags zur Zielerreichung und der Folgen der Nichterfüllung der Anforderungen bewusst.	

Lfd. Nr.	Ergänzende Anforderung	B
12	Die Organisation besitzt einen kontinuierlichen Verbesserungsprozess und erhält diesen aufrecht (lessons learned, Kommunikation, Prüfung der Wirksamkeit)	
13	Änderungsmanagement (geeignet, angemessen, wirksam)	
14	Sicherheitsmanagement (Informationssicherheit, Gebäudesicherheit etc.)	
15	Notfallmanagement	
16	Eskalationsmanagement	
17	Datenschutz	

Teil B – Spezielle Anforderungen an CSMS/SUMS

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Allgemeine Anforderungen und Planung des CSMS/SUMS					
Der Anwendungsbereich des CSMS/SUMS ist definiert; Ausschlüsse sind begründet und gerechtfertigt - Prozesse - Produkte - Standorte - Umgebung (z. B. Zulieferer, Ausgliederung)	7.2.2.1	7.1.1.1	D 1		
Das CSMS/SUMS umfasst alle Phasen. Die relevanten Prozesse (CS/SU im engeren Sinn und sonstige Prozesse) und Nahtstellen (auch zu externen Prozessen) sind ausreichend bzgl. CS/SU definiert; bestehende Prozesse und Nahtstellen wurden im notwendigen Umfang angepasst.	7.2.2	7.1.1	D 2		
Verantwortung der Leitung - Zu schützende Werte (Hardware, Software, Information) sind grundsätzlich für alle Phasen festgelegt - Politik und Ziele bzgl. CS/SU festgelegt (entsprechend den Gesamtzielen der Organisation) - Aufbau- und Ablauforganisation angemessen festgelegt - Überwachung organisiert, ausgewertet - Verantwortlichkeiten definiert - Verständnis/Bewusstsein für CS auf dem notwendigen Niveau gehalten - Ressourcen bereitgestellt - Verbesserung gefordert - Stabilität bei Änderungen gewährleistet usw.	7.2.2	7.1.1	A 1 9 10 11 12 17		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Der Informationsaustausch mit Typgenehmigungsbehörde und Technischem Dienst ist organisiert und wirksam	6.10	6.8	A 9 11		
Risikomanagement					
Zu schützende Werte sind im Detail für alle Phasen festgelegt. (u.a. für Software vor und während des Updates)	7.2.2.1	7.1.3 7.2.1.1 7.2.1.2	D 1 2 4 5 12		
Die Risikoanalyse und die daraus resultierende Planung des CSMS/SUMS werden als gelenkter Prozess durchgeführt - Verantwortlichkeiten - Definition - Überwachung/Aktualisierung usw.	7.2.2	7.1.1	D, A 3 6 9 10 11 12 13		
Es wurde eine umfassende Risikoanalyse durchgeführt - Quellen - UN-R 155 Anhang 5 bzw. UN-R 156 - Zu schützende Werte Schwachstellen - Angriffspfade und -szenarien - Interne/externe Faktoren - Vertraulichkeit, Integrität, Verfügbarkeit von Informationen Es wird dokumentiert begründet, wenn Maßnahmen nach UN-R 155 Anhang 5 nicht umgesetzt werden Details s. Checkliste „Risikoanalyse“	7.2.2.2 7.2.2.3 7.2.2.5 7.3.2 7.3.5	7.1.3.1 7.1.3.2 7.2.1.1 7.2.1.2	A 1 3 5 9 10 11 12 13 17		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Die Risikoanalyse umfasst für alle relevanten Standorte - Identifizierung - Auftretens- und Entdeckungs-wahrscheinlichkeit - Auswirkung/Kategorisierung - Bewertung anhand festgelegter und sinnvoller Kriterien - Priorisierung Details s. Checkliste „Risikoanalyse“	7.2.2.2 7.2.2.5 7.3.2	7.1.3.1 7.1.3.2 7.2.1.1 7.2.1.2	A 1 3 5 9 10 11 12 13		

Die Risikoanalyse bezieht sich auf
- Produkt (Fahrzeug)
  - Bauteile und Systeme
  - deren Zusammenwirken untereinander
  - Zusammenwirken des Fahrzeugs und seiner Einzelkomponenten/-systeme mit externen Systemen
  - Schutz vor unzulässigen (kompromittierten) Updates (UN-R 156)
- Prozess
  - Prozesse in der Organisation und deren Nahtstellen
  - Nahtstellen zu externen Prozessen
  - Prozesse in der Nachproduktionsphase
  - an allen relevanten Standorten
- Beteiligte Personen
- vom Hersteller zu berücksichtigende Infrastruktur und sonstige äußere Faktoren
- Softwareupdate (einschl. Backend und Fz), nur R-156
 	
Details s. Checkliste „Risikoanalyse“
	7.3.3
	7.2.2.2
	7.2.2.5
	7.3.2
		7.1.3.1
		7.1.3.2
		7.2.1.1
		7.2.1.2
			A
			1 3 5 9
			10 11
			12 13
			17		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B

Alle wesentlichen Schwachstellen werden erkannt, analysiert und ggf. behandelt
- Entwicklung
- Produktion
- Nachproduktion
- (Verschrottung)
- Softwareupdate
  - Systeme, Bauteile können ausgeschlossen werden, wenn sie nachweislich nicht updatefähig sind
  - Backend und Fz. sind einbezogen
	7.2.2.1
	7.2.2.2
	7.2.2.5
		7.1.3.1
		7.1.3.2
		7.1.3.3
		7.2.1.1
		7.2.1.2.3
			A
			5 9-13		

Es sind wirksame und angemessene Prozesse installiert, um in allen Phasen versuchte und erfolgreiche Angriffe - zu erkennen - den richtigen Stellen zeitgerecht auf angemessenen Kanälen zur Verfügung zu stellen - umfassend auf reale und potenzielle direkte und indirekte Auswirkungen zu analysieren - Maßnahmen für Produkt, Prozess und Vorbeugung abzuleiten und in einem vernünftigen Zeitfenster umzusetzen (u.a. wird die Risikoanalyse aktualisiert) - Wirksames Eskalationsmanagement - Softwarecode und -funktionalität wird nach dem Update verifiziert und validiert; unzulässige (kompromittierte) Updates werden unterbunden	7.2.2.2 7.2.2.3	7.1.3.1 7.1.3.2 7.1.3.3 7.2.1.1 7.2.1.2	D, A 1 2 4-6 8 9-16		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Aus der Risikoanalyse werden angemessene Maßnahmen abgeleitet. Das Risiko wird nach Festlegung der Maßnahmen neu bewertet und ist als akzeptabel eingestuft Die Wirksamkeit, Effektivität, Angemessenheit der Maßnahmen wird über einen angemessenen Zeitraum bewertet.	7.2.2.2	7	A 2 3 5 9-16		
Der gegenseitige Einfluss der Maßnahmen im Ergebnis der Risikoanalyse oder nach Vorfällen wird berücksichtigt	7.2.2.3	7	2 10-16		
Anforderungen an Prozesse (Details s. Checkliste)					
Produktentwicklung - Ziel - CS/SU-Anforderungen (im Entwicklungsauftrag/Lasten-/ Pflichtenheft) - Notwendige Eingaben - Steuerung des Entwicklungs-prozesses - Verifizierung/Validierung (ggf. auch für verschiedene Kombinationen von Modulen) - Dokumentation	7.2.2.2	7.1.1	D, A 1-6 9-16		
Die Konstruktion basiert auf der Risikoanalyse und dem zum Zeitpunkt der Genehmigung aktuellen Stand der Technik (z. B. kryptografische Module); wenn nicht, ist die Abweichung begründet	7.3.8	7.1.1	A 5 9-12		
Alle relevanten Prozesse bis einschließlich Produktionsphase sind ausreichend bzgl. CS/SU-Risiken bewertet und definiert (einschl. Produktion, Beschaf-fung, Wartung, Service usw.)	7.2.2	7.1.1	D 3 5 6 9-16		

Anforderung	UN-R		Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
	155	156			
Alle relevanten Prozesse der Nach-Produktionsphase (z. B. Wartung, Unfälle, Instandsetzung, Tuning, Softwareupdate, Verschrottung usw.) - sind ausreichend bzgl. CS/SU-Risiken bewertet und definiert - Die Wirksamkeit der im Produkt integrierten CS/SU-relevanten Eigenschaften wird überprüft/wiederher-gestellt (Schutz-, Datenüber-tragungsmechanismen usw. - Aufgaben der Marktüberwachung (z. B. Auslesen von Information über mögliche Angriffe) Während Servicetätigkeiten/ Reparatur wird das Risikoniveau nicht heraufgesetzt; vorhandene Informationsquellen werden genutzt (z. B. Auslesen von Speichern); Vertraulichkeit, Integrität und Verfügbarkeit bleiben beim Serviceprozess sowie bei der Übertragung von Information erhalten.	7.2.2.2 7.2.2.4 7.2.2.5	7.1.1	D 3 5 6 9-16		
In allen relevanten Prozessen ist die Sicherheit gewährleistet (Produktion, Lagerung, Wartung, Service usw.) Risiken bei Änderung der Prozesse oder der Prozesslandschaft sind abgesichert.	7.2.2.2	-	1 6 14		
Es existiert ein Prozess zur Prüfung (und Absicherung), dass over-the-air Updates während der Fahrt nicht die Sicherheit beeinträchtigen.	-	7.1.4.1	D 6 9,12 13 15 16		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Es ist prozessual abgesichert, dass das over-the-air Update nur ausgeführt wird, wenn ggf. notwendiges spez. Fachpersonal den Prozess unter Kontrolle hat.	-	7.1.4.2	A D 6 9 12 13 15 16		
Notwendige Prozesse (R-156) - Informationsmanagement - Softwareidentifikation und Sicherstellung der Integrität (einschl. relev. Hardware) - RXSWIN-Management (einschl. betroffener Soft- und Hardware) - Verifizierung der installierten Software in Bezug auf die RXSWIN (Aufbewahrung des eingefrorenen Softwarestandes für 10 Jahre nach Einstellung der Produktion) - Nachweis der Unabhängigkeit der Systeme mit Update von anderen - Identifizierung von Fahrzeugen, die das Update erhalten sollen - Bestätigung der Kompatibilität des Updates mit der Konfiguration des Zielfahrzeugs (spez. Software) vor dem Update-Start - Prüfung, ob durch das Update System-Typgenehmigungen betroffen sind (einschl. Identifizierungsparameter) (Aufzeichnungen zum Prüfprozess) - Prüfung, ob das Update Änderungen gegenüber dem ursprünglich genehmigten Fahrzeug bewirkt (Aufzeichnungen zum Prüfprozess)	-	7.1.1.1 7.1.1.2 7.1.1.3 7.1.1.4 7.1.1.5 7.1.1.6 7.1.1.7 7.1.1.8 7.1.1.9	A D 2 3 6 9 11-13 15 16		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
- Prüfung, ob das Update das sichere Verhalten und die Funktionalität des ursprünglich genehmigten Fahrzeugs beeinflusst (Aufzeichnungen zum Prüfprozess) - Information des Fahrers über das Update - Bereitstellung der Information über Softwareänderungen und betroffene Fahrzeuge für berechtigte Externe		7.1.1.10 7.1.1.11 7.1.1.12			
Update-Prozess - Prozessbeschreibung und Nachweise über Einhaltung der beschriebenen Prozesse - Beschreibung der Konfiguration jedes relevanten typgenehmigten Systems vor/nach dem Update (einschließlich eindeutiger Identifikation von Hard-/Software/Parametern) - Register mit Informationen zu jeder RXSWIN bzgl. Software vor/nach dem Update (auch alle relevanten Fz-/ Systemparameter) - Verzeichnis aller Ziel-Fz mit Bestätigung der Kompa-tibilität mit dem Update - Dokumentation des Updates (s. 7.1.2.5 a-i)		7.1.2 7.1.2.1 7.1.2.2 7.1.2.3 7.1.2.4 7.1.2.5	A D 2 3 6 9 11-13 15 16		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Sonstige Anforderungen gemäß UN-R 156					
RXSWIN - eindeutig identifizierbar - wird aktualisiert, wenn das Update typgenehmigungs-relevante Software betrifft - Schnittstelle zumindest über OBD-Schnittstelle leicht auslesbar (wenn RXSWIN nicht auf dem Fz. gespeichert wird: zumindest Meldung der Softwareversion an die Genehmigungsbehörde - gegen Manipulation geschützt (Maßnahmen sind der Genehmigungsbehörde geschützt mitzuteilen)	-	7.2.1.2	A D 5-16		
Over-the-air Update Anforderungen an das Fahrzeug - Bei nicht erfolgreichem Update kann der vorige Zustand hergestellt werden oder das Fz wird in einen sicheren Zustand gebracht. - Update nur möglich, wenn genug Energie vorhanden ist, dass Update abzuschließen und ggf. die Notfallmaß-nahmen (s.o.) auszuführen.	-	7.2.2.1	A D 5-16		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Over-the-air Update Zusätzliche Anforderungen - Bei sicherheitsrelevanten Updates wird das Fz durch techn. Maßnahmen in einen sicheren Zustand versetzt. - Der Fz-Nutzer wird vor dem Update gemäß 7.2.2.2 informiert. - Wenn das Update nicht während der Fahrt möglich ist, kann das Fz während des Updates nicht bewegt werden und der Fahrer kann keine potenziell gefährlichen Funktionalitäten nutzen. - Der Fz-Nutzer wird unabhängig vom Erfolg nach dem Ende des Updates informiert. - Der Fz-Nutzer wird über alle Änderungen und ggf. Änderungen zum Benutzerhandbuch informiert. - Das Fz. stellt sicher, dass alle Voraussetzungen vor Beginn des Updates erfüllt sind.	-	7.2.2.1 7.2.2.2	A D 5-16		
Extern bereitgestellt Prozesse, Produkte, Dienstleistungen					
Beurteilung, Auswahl, Leistungsüberwachung und Neubeurteilung externer Anbieter/ausgelagerter Prozesse - Festgelegt (Kriterien, Abläufe, Verantwortlichkeiten usw.) - Angemessen (entsprechend Risikoanalyse) - wirksam	7.2.2.5 7.3.2		D A 5 6 8- 12 14		
Klare und rechtlich verbindliche Beschreibung der zu erbringenden Leistung und der zu erfüllenden Sicherheitsmaßnahmen; angemessene Überprüfung der gelieferten Leistung	7.2.2.5 7.3.2		A 5 7 8 10-12		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Schutz der sicherheits-relevanten Information ist ausreichend organisiert und umgesetzt (beim Externen, beim Informationsaustausch).	7.3.2		1 9-12 14-16		
Überwachung und Messung (Details s. Checklisten)					
Sofern angemessen, werden Prüfungen geplant und durchgeführt in der - Produktionsphase - Nachproduktionsphase/ Service	7.3.5	7.1 7.2	D, A 6 7 9-13		
Wo notwendig, existieren Prüfanweisungen - zu prüfende Parameter - Prüfverfahren - Prüfmittel - Annahmekriterien Sie sind für den jeweiligen Anwender verständlich.	7.2.2.2 7.3.6	7.1 7.2	D 6 7 9-12 16		
Prüfergebnisse werden analysiert und ggf. Korrekturen/ Korrekturmaßnahmen erarbeitet und eingeleitet.	7.2.2.2 7.3.4	7.1.3.1 7.1.3.2 7.1.3.3 7.2.1.1 7.2.1.2.3	A 1 9-13 16		
Es existiert ein angemessenes Programm für interne CSMS/ SUMS-Audits, das umgesetzt wird und alle relevanten Bereiche und Standorte (einschließlich Service) umfasst; es werden Schwerpunkte gesetzt.	7.2.2.	7.1.1	D, A 1 5 6 9-12		
Es wird überwacht, dass der Lieferant die Vorgaben zur Gewährleistung von CS/SU einhält.	7.2.2.2 7.2.2.5 7.3.5	7.1.3.1 7.1.3.2 7.1.3.3 7.2.1.1 7.2.1.2	A 7-13 16		
CoP wird entsprechend dem Abkommen von 1958 sichergestellt. Ergebnisse werden aufgezeichnet und über den mit der Genehmigungs-behörde vereinbarten Zeitraum aufbewahrt.	9	9	A, D 7, 11-13		

Anforderung	UN-R 155	UN-R 156	Allg. Anforderung	Selbstauskunft des Herstellers/ *Vermerke des Auditors*/ der Auditorin *(kursiv)* (Verweise auf MS-Dokumente mit Angabe des Abschnitts möglich)	B
Die Marktüberwachung ist organisiert - Quellen (Fahrzeug, Nutzer, Servicebetriebe usw. - Verantwortlichkeiten - Meldepflichten, Meldewege - Schutz der Information - Auswertung; ggf. Maßnahmen und Anpassung der Risikoanalyse	7.2.2.2 7.2.2.5	-	A, D 1 3-6 9-16		
Feststellungsprotokolle und Verbesserungspotenzial der letzten Auditierung wurden ausreichend bearbeitet. Korrekturmaßnahmen sind effektiv.	7.2.2	7.1.1	A 1 10-13		
Sonstiges[4]					

[4] nur durch das KBA auszufüllen