

サイバーセキュリティ業務管理システム試験
(協定規則第 155 号 (同規則の規則 7.2. に限る))

1. 総則

サイバーセキュリティ業務管理システム試験の実施にあたっては、「自動車の特定改造等の許可に関する技術上の基準に関する細目等を定める告示」(令和 2 年国土交通省告示第 787 号)に定める「協定規則第 155 号の技術的な要件 (同規則の規則 7.2. に限る。)」の規定及び本規定によるものとする。

2. 試験条件

書面及び現地審査により試験を行うことができる。

3. 試験記録及び成績

試験記録及び成績は、付表の様式に記入する。

3.1. 当該試験時において該当しない箇所には斜線を引くこと。

3.2. 記入欄は、順序配列を変えない範囲で伸縮することができ、必要に応じて追加してもよい。

3.3. 試験記録及び成績は、日本語又は英語のみの記載でもよい。

付表

Attached Table

サイバーセキュリティ業務管理システム試験記録及び成績
CYBER SECURITY MANAGEMENT SYSTEM TEST DATA RECORD FORM
(協定規則第155号(規則7.2.サイバーセキュリティ業務管理システムに関する要件))
1958 Agreement of the United Nations Economic Commission for Europe Regulation No.155
(Restricted to paragraphs 7.2. Requirements for the Cyber Security Management System)

試験期日	年	月	日	試験担当者
Test Date	Y.	M.	D.	Tested by
<hr/>				
試験場所				
Test Site	<hr/>			

○ 改訂
Series

改訂番号
Series No.

補足改訂番号
Supplement No.

○ 試験対象業務管理システム
Test Management System

社名
Manufacturer

業務管理システムの名称
Names of Management System

○ 試験成績
Test Results

※ 各項目について適合性を裏付ける資料のリストを添付のこと。書式は任意で構わない。

Attach a list of supporting material for each paragraph. The format does not matter.

要件 Requirements		適合性 Conformity
段落 Paragraph	内容 Contents	
7.2.1.	For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.	
7.2.2.	The Cyber Security Management System shall cover the following aspects:	
7.2.2.1.	The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases:	
(a)	Development phase;	pass / fail
(b)	Production phase;	pass / fail
(c)	Post-production phase.	pass / fail
7.2.2.2.	The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:	
(a)	The processes used within the manufacturer's organization to manage cyber security;	pass / fail
(b)	The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered.	pass / fail
(c)	The processes used for the assessment, categorization and treatment of the risks identified;	pass / fail
(d)	The processes in place to verify that the risks identified are appropriately managed;	pass / fail
(e)	The processes used for testing the cyber security of a vehicle type;	pass / fail

	(f)	The processes used for ensuring that the risk assessment is kept current;	pass / fail
	(g)	The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified;	pass / fail
	(h)	The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks;	pass / fail
7.2.2.3.		The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2. (c) and 7.2.2.2. (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.	pass / fail
7.2.2.4.		The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2. (g) shall be continual. This shall:	
	(a)	Include vehicles after first registration in the monitoring;	pass / fail
	(b)	Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.	pass / fail
7.2.2.5.		The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.	pass / fail

備考

Remarks
