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:

h)  The **processes** used to **provide relevant data to support analysis** of attempted or successful cyber-attacks;

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that the process has been established to provide the data required for analysis to the department in charge of analysis (or the person who performs the analysis if the analysis is outsourced) |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Procedure for implementing SIRT activities (incidents)  -Field monitoring (obtaining information on incidents and vulnerabilities)  -Procedure when an incident occurs (Including an overview of what information is passed to the analyst in what steps)  -Procedure when vulnerability is discovered (Including an overview of what information is passed to the analyst in what steps) |

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.

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that after the identified risks have been classified, a process has been established to determine the response time limit based on the classification results.  Also, be able to explain the process by which OEMs take countermeasures when new threats or vulnerabilities are detected even after the development and production contract with the supplier has expired.  It is necessary to set the response deadline by processes such as triage and explain the monitoring process to see if it is executed within the deadline. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Procedure for implementing SIRT activities (incidents)  -Field monitoring (obtaining information on incidents and vulnerabilities)  -Procedure when an incident occurs  -Procedures for discovering vulnerabilities |

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;

(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.

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that utilizing the information on monitoring acquired in accordance with 7.3.7 and other manufacturer's storage, a process for utilizing the relevant data etc. for analysis shall be established. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Procedure for implementing SIRT activities (incidents)  -Field monitoring (obtaining information on incidents and vulnerabilities)  -Procedure when an incident occurs  -Procedures for discovering vulnerabilities |

**7.3. Requirements for vehicle types**

7.3.3 The vehicle manufacturer shall **identify the critical elements** of the vehicle type **and** **perform an exhaustive risk assessment** for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that risks shall be appropriately processed / managed by considering all threats including Annex5\_PartA and judging the necessity of countermeasures based on the results of risk analysis and risk evaluation. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

7.3.4. The vehicle manufacturer **shall protect the vehicle type against risks identified** in the vehicle manufacturer’s risk assessment. **Proportionate mitigations shall be implemented** to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

In particular, for type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.

1. **~~Implement appropriate cyber security measures~~** ~~in the design of the vehicle and its systems;~~

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that vehicle manufacturers implement appropriate mitigation measures in accordance with the need for measures based on the results of risk analysis and risk assessment. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Evidence that mitigation measures were introduced according to the necessity of measures (this includes:  ・the reason ,If mitigation measures other than Annex5 Part B and C are applied  ・the reason, If mitigation measures are determined to be unnecessary |

|  |
| --- |
| ~~Remark for test phase~~ |
|  |



7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

(a) detect and prevent cyber-attacks against vehicles of the vehicle type;

(b) support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;

(c) provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that the outline of the technology mounted on a vehicle in response to a cyber attack on the vehicle will be described.  (a): Attack prevention measures for vehicles are applied.  (b): The results of defense by vehicle manufacturer's preventive measures and monitoring results are recorded.  (c): The vehicle manufacturer should be able to read the recorded results and use them for analysis.  In any case, the outline of the technology shall be explained. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

7.3.8. Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.

|  |
| --- |
| Explanation of the requirement |
| The intent of this requirement is to ensure:  Regarding the points where encryption measures are taken based on the results of risk analysis and risk assessment,  (1) explain whether it complies with the consensus standard, and  (2) if it does not, explain the rational reason. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

7.4. Reporting provisions

7.4.1. The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.

|  |
| --- |
| Explanation of the requirement |
| The main purpose of this requirement is to confirm that the vehicle manufacturer runs CSMS related to the monitoring activities, as defined in paragraph 7.2.2.2.(g) properly after Development Phase. The manufacturer shall at least annually report to the Type Approval Authority who granted the type approval or the Technical Service who verified the compliance of its CSMS with this Regulation. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

7.4.2 The Approval Authority or the Technical Service shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.

If the reporting or response is not sufficient the Approval Authority may decide to withdraw the CSMS in compliance with paragraph 6.8.

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |