|  |
| --- |
| RDW Voertuiginformatie en -toelating |
| Report on Test Phase |
| UNECE Draft Regulation CS/OTA |
|  |
|  |
| **7/23/2019** |

|  |
| --- |
| Outcome of the Test Phase of the UNECE taskforce for cybersecurity and software updates |

This page is intentionally left blank

Table of Contents

[1. Stakeholders during the Test Phase 3](#_Toc14784882)

[2. Assessment steps during the Test Phase 3](#_Toc14784883)

[3. Document Topics 4](#_Toc14784884)

[3.1 Cybersecurity 4](#_Toc14784885)

[3.2 Software Updates 6](#_Toc14784886)

[4. Document Review 8](#_Toc14784887)

[4.1 Planning for Document Review 8](#_Toc14784889)

[4.2 Observations during Document Review of the Test Phase 8](#_Toc14784890)

[5. Onsite Assessment 10](#_Toc14784891)

[5.1 Proposed Schedule/Plan 10](#_Toc14784892)

[5.2 Observations during the Onsite Assessment 11](#_Toc14784893)

[5.2.1 Cybersecurity 11](#_Toc14784894)

[5.2.2 Software Updates 17](#_Toc14784895)

[6. Feedback to the Task Force 26](#_Toc14784896)

[6.1 General Feedback 26](#_Toc14784898)

[6.2 Enforcement of the Regulation 27](#_Toc14784899)

[6.3 Technical Services and Qualification 29](#_Toc14784900)

# Stakeholders during the Test Phase

Approval Authority

* RDW, Zoetermeer, The Netherlands

Technical Services

* UL B.V., Leiden, The Netherlands
* Secura B.V., Amsterdam, The Netherlands

Manufacturers- 4 vehicle manufacturers within the taskforce group

# Assessment steps during the Test Phase

These assessment steps have a generic nature for implementation. However, for each cluster, the steps were tailored to make the process of assessment as efficient and practical as possible. An assessment plan document was created and circulated between the clusters in order to provide guidance on the document topics owing to the redundancy of documents from individual regulation requirements. The document topics of the assessment plan are detailed in the below section.

# Document Topics

## Cybersecurity

The Cybersecurity Management System(CSMS) and Type Approval related set of document contents were expected to be delivered by the manufacturer to the Approval Authority and the Technical Services on a mutually agreed date, prior to the onsite assessment. Below is the basic list of documents for both CSMS and vehicle type but not an exhaustive list. Hence, submission of documents was not limited to the below list. The items in the list below could be converged in less number of documents as well, if desired by the Manufacturer.

* + 1. The documents for Vehicle Type should be delivered as per the Annex 1 of the latest draft regulation for GRVA-01-xx (UN TF-CS\_OTA) Final Draft Recommendation on Cyber Security incl. Annex A-D.
    2. The documents for CSMS should be delivered as below:
       1. Organization specific handbook for cybersecurity processes and activities *(or similar)* including commitment from the C-Level management for ensuring cybersecurity
       2. List of cybersecurity activities performed during Development, Production and Post-production phases
       3. Overall cybersecurity management with respect to each of the cybersecurity activities across Development, Production and Post-production phases.
       4. Cybersecurity principles implementation strategy including extended CIA
       5. Process of Risk assessment encapsulating, but not limited to, the below activities: -
          1. **Process for identification of the relevance of a system to cybersecurity**
          2. Process for description of the overall system with respect to Definition of the system/function, Boundaries and interactions with other systems, Architecture and environment of operation of the system *(context, constraints and assumptions)*
          3. Process of identification of assets and corresponding threats
          4. Process of assessing the impact for identified threats
          5. Process of identification of vulnerabilities, attack paths and corresponding attack feasibility
          6. Process of calculation, categorization and proportional treatment of risks
          7. Process to have residual risks within acceptable limits (organization) or else strong justification for non-adherence
          8. Process of acceptance of residual risks by stakeholders at appropriate levels of hierarchy.
          9. Processes used for keeping the risk assessments as current as possible
       6. Process for testing during development encapsulating the below activities not limited
       7. Extract of organization specific rules for testing during development *(from handbook)*
       8. Processes for creation and execution of test strategies
       9. Processes for execution of cybersecurity testing during system design, system development (Hardware and Software), system integration
       10. Processes for documentation of the results of testing
       11. Processes for handling vulnerabilities obtained during testing
       12. Processes for feeding back test findings into the development lifecycle
       13. Capability of the manufacturer to perform cybersecurity tests like Functional (requirement-based, positive and negative) testing, Interface testing, Penetration testing, Vulnerability scanning, Fuzz testing but not limited to the same. (state of the art tools and technologies)
    3. Process for testing during production encapsulating the below activities but not limited to -
       1. Processes for testing to ensure the produced system has the cybersecurity requirements, controls and capabilities outlined in the cybersecurity production plans
       2. Processes for testing to ensure the produced item meets the cybersecurity specifications which are in accordance with the system in the development phase.
       3. Processes for testing to assure that cybersecurity controls and configuration as cybersecurity specifications are enabled in the produced item.
       4. Processes for documenting the test results and findings handling
    4. Process of post-production encapsulating the below activities but not limited to -
       1. Cybersecurity monitoring program
          1. Process for identification of sources providing CS information on new and evolving cyber threats and vulnerabilities which was not anticipated to vehicle types during development and production
          2. Process for identification of sources from comparable industries or other threat sharing platforms.
          3. Process for cybersecurity information assessment (Identification of relevance of the collected information with respect to the system/vehicle of the manufacturer)
          4. Process for risk determination for the relevant information
          5. Process for identification of triggers for risk assessment for escalation to incidents
       2. Process for Incident response for identified high risk cyber attacks
          1. For already registered vehicles – incident response
          2. For vehicles not yet registered – adequate handling of such vulnerabilities
    5. Processes used in supply chain encapsulating the below activities but not limited to
       1. Organizational policy for supply chain
       2. Processes for incorporating risks originating from supply chain in risk assessment
       3. Processes for evaluation of supplier capability/certification of suppliers
       4. Processes to establish contracts, agreements for ensuring cybersecurity across the phases of development, production and post production
       5. Processes for cybersecurity assessment/audits of supplier cybersecurity activities
       6. Processes to ensure that the supply chain contains adequate measures to protect the integrity of software and hardware from suppliers during logistics and shipping.

## Software Updates

The Software Updates Management System (SUMS) and Type Approval related set of document contents were expected to be delivered by the manufacturer to the Approval Authority and the Technical Services on a mutually agreed date, prior to the onsite assessment. Below is the basic list of documents for both SUMS and vehicle type but not an exhaustive list. Hence, submission of documents was not limited to the below list. The items in the list below could be converged in less number of documents as well, if desired by the Manufacturer.

* + 1. The documents for Vehicle Type should be delivered as per the Annex 1 of the latest draft regulation for Final Draft Recommendation on Software Updates incl. Annex A-B.
    2. The documents for Software Update Management System (SUMS) should be delivered as below:
       1. For every new software update, existence of a –
          1. Target vehicles identification process
          2. Compatibility with existing hardware and other software process
          3. Impact assessment process *(assess, identify, record)* of software update on

Existing TA systems/parameters

Non TA systems (if affecting safety and continued operation of vehicle)

Adding/Altering or Enabling/Disabling any vehicle functionality

* + - * 1. Documentation *(record and store)* process for -

Overall software update processes

Relevant standards used

Configuration Management(CM) process including but not limited to

Unique Identification for software updates

Software Versions and configurations (initial and updated)

Affected hardware components

Integrity validation data

Interdependencies identification

Compatibility identification

* + - 1. Documentation (record and store) for each software update at vehicle type
         1. Target vehicle list(VIN level)
         2. Compatibility with registered /last known configuration
         3. Purpose of the update
         4. Impacted Systems/ Functions

Type Approved

Requirements of specific regulation

Parameters of specific regulation

Non Type Approved

* + - * 1. Safe and Secure execution

Conditions

Verification

* + - * 1. Intended functionality

Results of verification and validation

* + - 1. For RXSWIN
         1. Unique Identification process
         2. Document access by TA/TS
         3. Vehicular access through standardized ports
         4. Updating process for RXSWIN based on new TA or extension
         5. Verification of consistency of RXSWIN between vehicle and TA docs
         6. Protection against unauthorized modification (security of RXSWIN)
         7. Documentation

Associated software version

integrity validation data

* + - 1. Security of software updates
         1. Protection (Authenticity and Integrity demonstration) against

Manipulation during SU process

Compromise of development process

* + - * 1. Verify functionality and code
      1. Over the air updates
         1. Safety impact during driving

Restricted mobility

Reduced functionality

* + - * 1. Additional conditions for OTA

Power

Informing the user

Before Update- Information regarding update

After update- Success/ Failure of update

* + - * 1. Failure recovery

Rollback

Safe State

# Document Review



## Planning for Document Review

The below activities were performed during the document review planning phase of the test phase:

* + 1. Every document provided by the manufacturer was mapped into respective items outlined in the [section 3](#_Document_Topics) and corresponding coverage of the aspects was provided by the vehicle manufacturer.

* + 1. Absence of a document or expected contents of the documents was also reported by the manufacturer with adequate justification/clarification. The technical services reviewed and verified the completeness of the provided documentation as well as declared whether additional documents were required.
    2. Intra-evaluation of the documents within the respective organizations of the technical service and approval authority independently was performed and later on, Cooperative evaluation jointly by the approval authority and technical services after the intra-evaluation.
    3. The overall summary of each document (of manufacturer) along with TS’s perspective was presented to approval authorities by the technical services.
    4. Focus areas are areas of relevance based on adequacy of information provided, interpretation of the information provided as well as absence of any information provided by the manufacturer to TS/AA. Common understanding on focus areas was reached among the parties and a schedule for the onsite assessment was done over several online meetings between manufacturers, TSs and RDW.
    5. Examples of focus areas selected were risk management, cybersecurity monitoring, incident response etc.
    6. An intermediate report of the document review was prepared by the technical service before the start of the onsite assessment for stakeholders to be on the same page.

## Observations during Document Review of the Test Phase

* + 1. Majority of the manufacturers provided documentation to the technical services and RDW, prior to the on-site assessment. This enabled the TS and AA to perform an in-depth review of the documentation which later on provided inputs for defining an audit plan.
    2. Considering the fact that an in-depth look inside the documents was performed, the technical services and RDW were able to focus their attention during the audit exclusively on interviewing relevant persons, and validating that the processes/activities/evidence detailed in the documentation is actually in place.
    3. The documents provided by manufacturers were completely different in terms of structure, format and content topics. Hence, considerable effort was required to reconcile the purpose of the documents even though document review was a repeat procedure considering four of the manufacturers evaluated by RDW during this test phase.
    4. Certain manufacturers provided insufficient documents against the expectations outlined in section 3. This could be owing to limited amount of time for assessment, or light documentation processes for the manufacturers.
    5. For certain manufacturers, documents were provided in form of presentations and lacked the explanation for the process behind the pictorial representations in the slides. Technical details were missing from the documentation package. Only high level information was made available.
    6. For certain manufacturers, documents were incomplete in nature due to work in progress for a number of processes within the CSMS/SUMS. Certain documents were conceptual in nature like RXSWIN
    7. Certain manufacturers did not make available their documents due to the confidential nature of those documents. This prevented TS/AA to understand and reconcile the content of the documents. A live walkthrough of the documents was provided by the manufacturer but considerably difficult to understand the crux of those documents.
    8. Documents received from certain manufacturers were in a different language than English, and indeed a challenge for the non-native speakers of TS/AA
    9. Cybersecurity/Software Updates handbook was not provided to TS/AA as per the requirements of the assessment plan. And hence, this provides evidence that a formalized process for CSMS/SUMS may be non-existent as yet.
    10. Sample supplier contracts with cybersecurity clauses were not provided in the documentation package.
    11. Abstract/Redundant nature of the regulation requirements also posed as a hindrance for identifying the correct and required documents to be provided by the manufacturer. E.g. Treatment of risk vs Managing of risk
    12. There are a number of existing processes within the manufacturers and they essentially contribute to the CSMS/SUMS within the organization. But, they are not in line with the requirements of the regulation but act as pillars for establishment of the CSMS/SUMS. Documentations for those generic processes were written before the start of the pilot project and acted as a background to the requirements of the regulation.

# Onsite Assessment

## Proposed Schedule/Plan

The table below provides an example of on-site assessment schedule for manufacturers. The schedule addresses the relevant topics covering both the Cybersecurity as well as the Software Updates regulations.

Table 1: Sample Schedule for Onsite Assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Day 1 | Day 2 | Day 3 | | Day 4 | Day 5 |
| **Software Updates** | | | **Cybersecurity** | | |
| Introduction to Software Updates | Management solutions for software updates | Software updates: Practical example | | Cybersecurity: E/E security processes and handbook | Cybersecurity: Enterprise processes |
| Overview of IT Systems for software updates | RXSWIN | Software updates: Feedback and summary | | EE/A security processes application | Cybersecurity: Supply chain |
| Software update  a. Development process  b. handbook  c. Homologation of software updates | Security of Software Updates | Cybersecurity: Risk management process | | Cybersecurity: Field processes and handbook | Cybersecurity: Production security processes |
| Software updates Compatibility | Over the air Updates | Cybersecurity: Field processes application | Cybersecurity: Penetration testing, functional testing |
| Software updates: Version management | Debriefing | Debriefing | | Cybersecurity: Security testing - hackathons | Debriefing and closing |
| Preparation and implementation measures in the field | Debriefing | Debriefing |
| Debriefing |

## Observations during the Onsite Assessment

### Cybersecurity

|  |  |  |
| --- | --- | --- |
| **Req #** | **Requirement text** | **Observations during the audit (observation/recommendation/objective)** |
| **Requirements for the CSMS** | | |
| 7.2.1. | 7.2.1 For the preliminary assessment the Approval Authority or Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation. | **Observations:** It is not clear for the OEMs which processes are part of the CSMS |
| **Recommendation:** Would be useful to have a list of criteria on which below processes are needed to be in place. |
| **Objective:** To have an internal handbook and/or guidance text for Cybersecurity of the product |
| 7.2.2.1. | The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System considers the following phases:  - Development phase;  - Production phase;  - Post-production phase. | **Observations:** In development and post production, security activities seem to mostly in place and feasible. For production, activities do not focus on security, but on functional validation at the end of the line. The separation between development, production and post productions is not always clearly separated from each other. inside the OEMs. |
| **Recommendation:** |
| **Objective:** To check for existence of the cybersecurity activities in each of the 3 phases. |
| 7.2.2.2. | The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered. This shall include: | Requirements addressed in the lines below |
| 7.2.2.2 (a) | The processes used within the manufacturer’s organization to manage cyber security; | **Observations**: For some OEMs the processes are in a draft phase, and ISO 21434 is used as a basis. For some other OEMs, the processes have a lower maturity level and are based on a more ad-hoc basis. |
| **Recommendations**: Requirement is clear. |
| **Objective**: The objective of the requirement is the OEM has a governance process in place, like defining management roles, and these roles being followed in practice. |
| 7.2.2.2 (b) | The processes used for the identification of risks to vehicle types; | **Observations**: The processes exist, but the maturity level and the documentation of the process does not always exist. There are tools which the OEMs are using, but is of a certain subjective nature, with varying inputs for risk assessments. Every OEMs do risk analysis, but not in a structured and documented way. |
| **Recommendations**: To agree on what is the minimum criteria to evaluate risk assessment. |
| **Objective**: The objective is to see a standard process to identify all threats for a vehicle |
| 7.2.2.2 (c) | The processes used for the assessment, categorization and treatment of the risks identified; | **Observations**: The processes exist, but the maturity level and the documentation of the process does not always exist. There are tools which the OEMs are using. Every OEMs do risk analysis, but not in a structured and documented way. The scales are different for OEMs. |
| **Recommendations**: To agree on what is the minimum criteria to evaluate risk assessment. |
| **Objective**: The objective is to see that all the risks are categorized and treated based on this classification. How the risks are escalated to the higher management and how often is the management informed. |
| 7.2.2.2 (d) | The processes in place to verify that the risks identified are appropriately managed; | **Observations**: Acceptance of risks is done by the same department which identifies the risks, and not by a higher level |
| **Recommendations**: To agree on what is the minimum criteria to evaluate risk assessment. The minimum process which needs to be in place. |
| **Objective**: Objective is to have a methodology for risk acceptance (including residual risks) including how the management sign of |
| 7.2.2.2 (e) | The processes used for testing the security of the system throughout its development and production phases; | **Observation**: Security testing is not very common for the OEMs, but there are exceptions. There is an inherent intention of the OEMs to have a security testing competencies, or to outsource this to test parties. |
| **Recommendation**: To have an in-house resources with good knowledge. |
| **Objective**: To ensure the requirements are in place and working as expected. Motivation/Justification to be provided on the way of performing testing and does it ensure coverage of the cyber risks. |
| 7.2.2.2 (f) | The processes used for ensuring that the risk assessment is kept current; | **Observation:** There are no triggers to keep the risk assessment current unless there is replacement of components or change in architecture. Cybersecurity events are tracked through tickets and then risk assessment is reiterated for some manufacturers. |
| **Recommendation:** There should be periodic evaluations or specific triggers mandated by the regulation to have certain triggers for keeping risk assessment current. Time limit recommendation is not realistic. |
| **Objective:** Lessons learned from Incident response and also development process or similar are incorporated back into the risk assessment to keep it current. |
| 7.2.2.2 (g) | The processes used to monitor for, detect and respond to cyber-attacks on vehicle types; | **Observation:** Monitoring is very passive in majority of manufacturers and active detections have to be performed. Some manufacturers have active tamper detections inbuilt in their vehicles. Some other manufacturers lack a monitoring process as such.  Triaging is performed on the cybersecurity information obtained during the passive monitoring (also from active if present).  Incident response is not streamlined and response requirements are not standardized. There is no harmonized understanding of what is meant by Incidents across manufacturers. |
| **Recommendation**: Active monitoring (Ex-Intrusion detection systems) should also be incorporated in the vehicles itself to monitor vehicle related attacks which are unpublished yet conducted by malicious actors. The regulation should drive to characterize the incidents (specific labelling for differentiating incidents and events) and corresponding response across the industry. |
| **Objective**: To check for existence of process for active and passive cybersecurity monitoring, triaging process for converting information into event/incident and appropriately respond to incidents. There should be clear differentiation between normal and high critical vulnerabilities and incidents. |
| 7.2.2.2 (h) | The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types; | **Observation:** Hackathons are performed but not regularly. Frequency has to be increased. Some manufacturers support bug bounty programs and hackathons. They provide active support to drive the research by third parties. Some other manufacturers are lacking a process of checking the evolving threats and vulnerabilities. |
| **Recommendation**: Vulnerability management needs to be in place during the entire lifecycle. |
| **Objective**: Penetration testing, bug bounties or hackathons are being performed by the manufacturers or similar to keep up with the changing threat landscape. |
| 7.2.2.2 (i) | The processes used to appropriately react to new and evolving cyber threats and vulnerabilities. | **Observations**: Majority of manufacturers do the response in the standard incident response process. However, an active monitoring is still required in order to respond to such new and evolving threats. |
| **Recommendation**: Vulnerability management needs to be in place during the entire lifecycle. |
| **Objective**: A vulnerability management process which takes care of vulnerabilities as and when it is detected for new and evolving threats. |
| 7.2.2.3. | The vehicle manufacturer may refer to [the Recommendation / Resolution on cyber security] when describing the processes they have employed. |  |
| 7.2.2.4. | The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers and service providers in regards of the requirements of paragraph 7.2.2.2. | **Observations**: Suppliers are audited frequently but not focused on cybersecurity. Supplier selection requires certain certifications common across automotive industry. Auditing in terms of integrating the CSMS of supplier. Transferring materials/components to supplier to OEM is not structured. Validating the cybersecurity requirements of the packages received from supplier is not common in many manufacturers. Integrating ISO/SAE 21434 with ASPICE model for cybersecurity evaluation of suppliers. |
| **Recommendations**: What aspects of the supply chain management has to be considered in the evaluation? Clarity can be provided on this. There is no requirement to have suppliers of manufacturers in scope. That is under scope of the manufacturer. Risks related to supply chain needs to be included in the risk assessment of the manufacturer. |
| **Objective:**  - They have qualification requirements for suppliers (certification and audit),  - Threats, Vulnerabilities and Risk assessments for cybersecurity and integrating information(CSMS) from suppliers  - Receiving and validating inputs from suppliers |
| **Requirements for the vehicle type** | | |
| 7.3.1. | Before the assessment of a vehicle type for the purpose of type approval is carried out the vehicle manufacturer shall demonstrate to the Approval Authority or Technical Service that their Cyber Security Management System has a valid CSMS Certificate of Compliance relevant to the vehicle type being approved. | **Observations/Questions:** This requirement was not validated during the test phase. But the overall question and understanding remains on the following:   * 1. Does the TS go through the entire risk assessment of individual functions/components?   2. Does the TS go through the entire risk assessment of complete vehicle?   3. Is exhaustive evaluation of every function/component of the vehicle required?   4. If yes, it is impossible to do it during a short time frame of assessment. |
| 7.3.2. | The Approval Authority or Technical Service shall verify that the manufacturer has taken the necessary measures relevant for the vehicle type to:  (a) Collect and verify as appropriate information required under this regulation, through the full supply chain;  (b) Maintain appropriate design and test information;  (c) Implement appropriate security measures in the design of the vehicle and its systems; |
| 7.3.3. | The vehicle manufacturer shall demonstrate the risk assessment for the vehicle type in terms of the vehicle systems, the interactions of the different vehicle systems and the entire vehicle. | **Recommendation:** Be very specific on what needs to be done in the type approval and a general clarity has to be provided in the regulations. The requirements should be more objective on the type approval of the vehicle.  Example - How to demonstrate the risk assessment for the vehicle type in terms of the vehicle systems, the interactions of the different vehicle systems and the entire vehicle in an auditable and useful manner. The level of detail should be harmonized. |
| 7.3.4. | The vehicle manufacturer shall demonstrate how the design of critical elements of the vehicle type are protected against risks identified in the vehicle manufacturer’s risk assessment. Proportionate mitigations shall be implemented to protect such elements |
| 7.3.5 | The vehicle manufacturer shall demonstrate how they have implemented appropriate and proportionate measures to protect dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data. | **Objective**: To assess the specific documentation for a vehicle type |
| 7.3.6. | The vehicle manufacturer shall describe what testing has been performed to verify the effectiveness of the security measures implemented and the outcome of those tests. |

### Software Updates

|  |  |  |
| --- | --- | --- |
| Req# | Requirement text | Observations during the audit (observation/recommendation/objective) |
| **Requirements for the SUMS** | | |
| 7.1.1.1. | A process whereby information relevant to this regulation is documented and securely held at the vehicle manufacturer and can be made available to an Approval Authority or Technical Service upon request without any burden; | **Observation**: Some manufacturer had reservations about sharing sensitive information with the TS/AA. |
| **Recommendation**: Need clarify on what is meant by “securely held”. Also explicitly clarify what information needs to be stored by the manufacturer and what needs to be shared with TS/AA. To be clarified in each of the below requirement, if not already done. |
| **Objective**: |
| 7.1.1.2. | A process whereby information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified; | **Observation**: Software versions are documented, there is a process for identifying the same.  Integrity validation data not uniformly understood across the OEMs, not implemented by all manufacturers. CAL\_ID/ CVN concept, which is used for emission software, to be extended for use for software updates.  Hardware versions are well documented as per the regulation. |
| **Recommendation:** Have a harmonized understanding of “integrity validation data” |
| **Objective:** To check the existence of software versions, integrity validation data and hardware version/ component number/part number, and the traceability between them |
| 7.1.1.3. | A process whereby, for a vehicle type that has an RXSWIN, information regarding the RXSWIN of the vehicle type before and after an update can be accessed and updated. This shall include the ability to update information regarding the software versions and their integrity validation data of all relevant software for each RXSWIN. | **Observation**: RXSWIN is still in a concept level for all manufacturers.  Some manufacturer also questions the intention of using the RXSWIN, as long the constituents of the RXSWIN like SW versions, IV data etc. are present |
| **Recommendation**: RXSWIN is a mandatory requirement. Amend the requirement “for a vehicle type that has an RXSWIN”, and make the requirement concrete. |
| **Objective:** Effectively check the existence of RXSWIN, information regarding the RXSWIN of the vehicle type before and after an update in the OEMs backend. |
| 7.1.1.4. | A process whereby, for a vehicle type that has an RXSWIN, the vehicle manufacturer can verify that the software version(s) present on a component of a type approved system are consistent with those defined by the relevant RXSWIN; | **Observation**: Verification to be done through standardized means like the OBD port. For some manufacturers, they rely on the vehicle to check the reliability of the software version, and not explicitly verify the same. They rely on the fact that their implementation of the solution is tamper proof, so software version “has to be” consistent with the RXSWIN. Some manufacturer enforces the same by ensuring only signed software to be installed in the vehicle. |
| **Recommendation**: |
| **Objective**: Check the implementation of RXSWIN and the corresponding software versions, and ensure its traceability. Also check for a one-to-one mapping between the RXSWIN in the vehicle and the manufacturers backed and type approval documents. |
| 7.1.1.5. | A process whereby any interdependencies of the updated system with other systems can be identified; | **Observation**: Interdependency check present among manufacturers for hardware and software is present. Scope/ extent of interdependency check was not clearly demonstrated by some manufacturers. OEMs gave a statement of confirmation that it is checked  Interdependencies are checked more at the engineer level, who develops the system, but not at the TA/homologation level.  Some manufacturer refused to disclose this information. |
| **Recommendation**: Clarify how the requirement needs to be demonstrated and ensure that OEMs make available this information for verification by the TS. |
| **Objective**: Verify interdependencies at every level (vehicle, system, SW-HW, SW-SW, HW-HW level) |
| 7.1.1.6. | A process whereby the vehicle manufacturer can identify target vehicles for a software update; | **Observation**: Most Manufacturer implements this requirement in a mature way, some in a very immature level. |
| **Recommendations**: |
| **Objective:** |
| 7.1.1.7. | A process to verify, before a software update is issued, the compatibility of possible software/ hardware configurations for the registered configuration or last known configuration of the target vehicles with the software update; | **Observation**: Compatibility check is performed at the development level, installation is allowed only if the compatibility check is performed as a pre requisite.  Most manufacturer performs only wired updates, for which compatibility check is a check to be verified. |
| **Recommendations**: Clarify how the requirement needs to be demonstrated and ensure that OEMs make available this information for verification by the TS. |
| **Objective**: Verify hardware/software compatibility before the update execution. |
| 7.1.1.8. | A process to assess, identify and record whether a software update will affect any type approved systems. This shall consider whether the update will impact or alter any of the parameters used to define the systems the update may affect or whether it may change any of the parameters used to type approve those system (as defined in the relevant legislation); | **Observation**: Most manufacturer has a formal homologation process to identify TA impacts.  Some manufacturer is not clear of a minor/ major change, or its possible combinations to consider for a TA impact. |
| **Recommendations**: |
| **Objective**: |
| 7.1.1.9. | A process to assess, identify and record whether a software update will add, alter or enable any functions that were not present, or enabled, when the vehicle was type approved or alter or disable any other parameters or functions that are defined within legislation. The assessment shall include consideration of whether:  (a) Entries in the information package will need to be modified  (b) Test results no longer cover the vehicle after modification | **Observation**: Most manufacturer has a formal homologation process to identify TA impacts.  Some manufacturer is not clear of a minor/ major change, or its possible combinations to consider for a TA impact. |
| **Recommendations**: |
| **Objective**: |
| 7.1.1.10. | A process to assess, identify and record if a software update will affect any other system required for the safe and continued operation of the vehicle or if the update will add or alter functionality of the vehicle compared to when it was registered; | **Observation**:  Some manufacturer ensures only required functions are present in the vehicle, but the vehicle is issued for TA on its full scope of functions. Based on paid service model, functionalities are activated/ deactivated. OEMs claims/ ensures this model of work is followed for all TAs |
| **Recommendations**: |
| **Objective**: |
| 7.1.1.11. | A process whereby the vehicle user is able to be informed about updates. | **Observation**: Some manufacturer informs only the fleet owner about the update; and the end user is only informed of the installation info.  Manufacturer do not have a harmonized way of informing the users |
| **Recommendation**:  Have a clear list of a minimum set of info which the OEM needs to inform the user. |
| **Objective** |
| 7.1.1.12. | A process whereby the vehicle manufacturer shall be able to make the information according to paragraph 7.1.2.3. and 7.1.2.4. available to relevant Authorities or Technical Services. | **Observations**: |
| **Recommendations**: |
| **Objective** |
| 7.1.2. | The vehicle manufacturer shall record, and store at their premises, the following information for each update applied to a given vehicle type: | Addressed in the requirements below |
| 7.1.2.1. | Documentation describing the processes used by the vehicle manufacturer for providing software updates and any relevant standards used to demonstrate their compliance; | **Observation**: Documentation regarding the process of delivering software updates is generally in place with the OEMs. Documentation regarding the development of software updates is missing in some cases, the process is less mature.  No relevant standards were demonstrated during the assessment by the manufacturers. |
| **Recommendations**:  Clarify if providing means development and testing, delivery and installation the updates |
| **Objective**: See the process for developing and delivering software updates documented |
| 7.1.2.2. | Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identifiers for the type approved system’s hardware and software and any relevant vehicle or system parameters; | **Observation**: OEMs have internal databases (tools) in which they can track the configuration of the vehicles (and their systems) before and after the update.  Specific firmware is meant for ECUs for certain manufacturers and a configuration for each ECU(Component) is maintained. Other manufacturers have a whole vehicle based software.  Documentation can be generated from the internal tooling for the configuration management. |
| **Recommendation**: To clarify what is meant by configuration, and what exactly do OEMs need to have in place. |
| **Objective**: To see a database with the vehicle types, and for each hardware/software component under that type, the previous and new software versions and corresponding documentations as well. |
| 7.1.2.3. | For every RXSWIN, there shall be documentation describing the software relevant to the RXSWIN of the vehicle type before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software for each RXSWIN. | **Observation**: RXSWIN is mostly not implemented within the OEMs |
| **Recommendation**: Integrity validation data is ambiguous. Verification/Use case associated with the integrity validation data has to be made or clarified(*this is mostly handled under requirement 7.1.3)*. Approval authorities or TS can’t really verify the software version from the integrity validation data. The purpose of usage of integrity validation data is not present. |
| **Objective**: There should be a way to see for all the types the RXSWINs associated with that type, and all the software versions under that RXSWIN. This should also include integrity validation data for the software versions. |
| 7.1.2.4. | Documentation listing target vehicles for the update and verification of the compatibility of the registered configuration or last known configuration of those vehicles with the update. | **Observation**:  All manufacturers have a method/tool for determining the last known configuration for vehicles on the field/under production. The validation of compatibility is mostly performed by the update tool or by the vehicle itself, and sometimes are not documented by the manufacturers. The actual configuration of the vehicle is determined *(in garage)* once it reaches the dealer post a campaign for update. If compatible, the update is performed. For OTA updates, the configuration of the vehicle determines if a new update will be installed or not. Some manufacturers roll out the update in groups of vehicles instead of doing it at once in order to manage the update process better. |
| **Recommendation**: It has to be clear what kind of evidence is needed in order to show the compatibility/test coverage with all configurations. Are test reports sufficient, or do we need something more explicit? |
| **Objective**: For each software update, there should be a traceable way to check the target vehicles in scope of the update as well as list the hardware components impacted by the update. It should be traceable by the manufacturer/vendor and auditable by TS. |
| 7.1.2.5. | Documentation for all software updates for that vehicle type describing:  (a) The purpose of the update;  (b) What systems or functions of the vehicle the update may  (c) Which of these are type approved (if any);  (d) If applicable, whether the software update affects any of the relevant requirements of those type approved system;  (e) Whether the software update affects any system type approval parameter;  (f) Whether an approval for the update was sought from an approval body;  (g) How the update may be executed and under what conditions;  (h) Verification that the software update will be conducted safely and securely.  (i) Verification that the software update has undergone adequate verification and validation procedures. | **Observation**: The purpose of the update, as well as the impact on other systems is considered, but not always documented in a clear way. Impact on the type is not always considered and documented, the processes are not mature for some manufacturers.  Requirement a)- clear documentation available  Requirement b)- Architecture dependent, manufacturers not clear on the extent of impact to be documented.  Requirement c), d) - Normal homologation process, manufacturers are clear on this requirement.  Requirement e)- - Normal homologation process, manufacturers are clear on this requirement.  Requirement f)- - Normal homologation process, manufacturers are clear on this requirement.  Requirements g), h)– Documentation is present in a general way, but not for each update. Instructions are given to the respective technician in the garage on how to perform the update  Requirement i)- Manufacturers doesn’t have documentation for the verification process yet, but the process is incorporated in the development process. |
| **Recommendation**: Make it clear if exact documentation detailing the purpose, impacted systems, type approval impact, verification of software validation and all the rest need to be documented in dedicated documents, or this can be kept as part of the development cycle. Also, do the OEMs need to share this information with TS for validation?  Clarify that this requirement is about documenting a general process of how the update will be performed as per the sub requirements , with a demonstration of the same while approving an actual vehicle type.  Requirements c),d),e) and f can be combined to a single requirement.  Requirement h) is redundant detailed in further requirements below in 7.1.3 and 7.1.4. |
| **Objective**: To validate the existence and consistency of documentation for all the above mentioned categories |
| **7.1.3.** | **Security, the vehicle manufacturer shall demonstrate:** | |
| 7.1.3.1. | The process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated; | **Observation**: The protection of the software updates process is mostly in place, by either means of signatures or secure pairing to the software updates server.  Software updates are kept in secure target locations which are under the control of the OEMs before being sent to the vehicles. |
| **Recommendation**: to make clear if a specific security control is needed here (e.g. signatures must always be used, or this can be kept flexible to the OEMs. Also, to TS need to go in depth during the assessment of the implemented security control?  Does the TS audit needs to cover the process of transferring the update package from the supplier? |
| **Objective**: To assess the way in which software updates are protected while being sent to the vehicle (including updates received from the suppliers) and determine if this is sufficient. Also to assess how software updates are stored before the update process is started |
| 7.1.3.2. | The update processes used is protected to reasonably prevent it being compromised, including development of the system update; | **Observation**: In most of the cases, the controls for this requirement are achieved in the same way as for the previous requirement. E.g. signatures are in place, which prevent the software images from being modified.  Manufacturers have different means of procuring the software from the supplier, specifics on how the procurement is done is not well documented. Manufactures don’t have complete visibility on how the software is procured securely for all instances. |
| **Recommendation**: To clarify if specific controls are intended to be verified here, or this can be flexible depending on the implementation of the OEMs  Does the TS audit needs to cover the process of transferring the update package from the supplier?  Not clear what criteria has to be used to test this requirement. Security Testing, integration testing and its coverage are not mentioned. Objective criteria to be described on what testing needs to be done and how test coverage is ensured. |
| **Objective**: To assess the possibility of replacing the updates with a malicious one, and attempting to send this malicious update to the vehicle. |
| 7.1.3.3. | The processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate. | **Observation**: Testing of the software updates is in place during the development phase. Testing does not in general include security testing.  Manufacturers where unclear if the source code verification needs to be validated by the TS. |
| **Recommendation**: Make it clear if TS need to access and assess test reports.  Not clear what criteria has to be used to test this requirement. Security Testing, integration testing and its coverage are not mentioned. Objective criteria to be described on what testing needs to be done and how test coverage is ensured. |
| **Objective**: Verify that a testing/validation process is in place for the software updates, and validate that the performed tests cover the functionality of the update. |
| 7.1.4. | Additional Requirements for Software Updates over the air | |
| 7.1.4.1 | The vehicle manufacturer shall demonstrate the processes and procedures they will use to assess that over the air updates will not impact safety if conducted during driving. | **Observation**:  No manufacturer perform updates that affects safety while driving. |
| **Recommendation**: Are there any specific conditions which always need to be in place for ensuring safety of vehicle when update is conducted during driving? |
| **Objective**: Determine and analyze the conditions required by the OTA installation, to ensure that the safety while driving is not impacted |
| 7.1.4.2. | The vehicle manufacturer shall demonstrate the processes and procedures they will use to ensure that, when an over the air update requires a skilled person, such as a mechanic, in order to complete the update process, the update can only proceed when such a person is present. | **Observation**: This depends per OEM. Generally, they don’t require additional support for the OTA update, but just in the case of an error during the update.  Update mechanism doesn’t generally require a skilled person while updating. The responsibility of properly installing the update is never left to the user/driver. Incase an error is encountered, manufacturer support is requested to complete the installation of the update. |
| **Recommendation**: Make it clear under which circumstances an update would require the assistance of a skilled person.  Make the intention of the requirement to specify that the user is not able to perform an update incase external assistance is required. Updates can either be of the type where the vehicles install the update by itself, or it is performed under the manufacturers control. |
| **Objective**: To check which types of OTA updates require the assistance of a person, and how is this process implemented. |
| **Requirements for the vehicle type (observations below are more theoretical / based on a non-type approved system)** | | |
| 7.2.1.1. | The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates. | **Observations**: Protections for the software updates are in place per OEMs, different approaches exist. |
| **Recommendation**: Do the TS need to assess the way in which the integrity of software updates is implemented, more than just mentioning the control in place? |
| **Objective**: To check the way in which the integrity is ensured during the process, and assess if the implemented control is sufficient |
| 7.2.1.2.1 | Each RXSWIN shall be uniquely identifiable. When type approval relevant software is modified by the vehicle manufacturer, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval. | **Observations**: RXSWIN is mostly not implemented with the OEMs |
| **Recommendation**: To make it clear if the RXSWIN specification must be implemented by the OEMs |
| **Objective**: To check the process and documentation on how the RXSWIN was updated for a vehicle type |
| 7.2.1.2.2 | The RXSWIN shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port). | **Observations**: RXSWIN is mostly not implemented with the OEMs |
| **Recommendation**: Some OEMs prefer to display the RXSWIN information on the screen, not via the OBD port. To state in the requirement that alternative ways of displaying the RXSWIN are acceptable. Is the OBD port retrieval mandatory? |
| **Objective**: Confirm that the RXSWIN can be retrieved from the vehicle |
| 7.2.1.2.3. | The vehicle manufacturer shall protect the RXSWINs on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the | **Observations**: RXSWIN is mostly not implemented with the OEMs |
| **Recommendations**: |
| **Objective**: To assess the way in which the RXSWIN information is stored on the vehicle |
| **7.2.2.1** | **The vehicle shall have the following functionality with regards to (over the air) software updates:** | |
| 7.2.2.1.1 | The vehicle manufacturer shall ensure that the vehicle is able to restore systems to their previous version in case of a failed or interrupted update or that the vehicle can be placed into a safe state after a failed or interrupted update. | **Observations**: OTA is mostly not implemented in the OEMs. Where implemented, this requirement seems to be met. |
| **Recommendations**: |
| **Objective**: Assess that rollback is implemented, or the existence of a safe state |
| 7.2.2.1.2. | The vehicle manufacturer shall ensure that software updates can only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state). | **Observations**: OTA is mostly not implemented in the OEMs. Where implemented, this requirement seems to be met. |
| **Recommendations**: |
| **Objective**: Confirm that the OTA process does include a validation for sufficient power |
| 7.2.2.1.3. | When the execution of an update may affect the safety of the vehicle, the vehicle manufacturer shall demonstrate how the update will be executed safely. This may be achieved through technical means and/or through a process that will require the vehicle user to provide verification that the vehicle is in a state where the update can be executed safely. | **Observations**: OTA is mostly not implemented in the OEMs. Where implemented, this requirement seems to be met. |
| **Recommendations**: |
| **Objective**: Confirm that the OTA process does include a validation of safe conditions for installing the update |
| 7.2.2.2 | The vehicle manufacturer shall demonstrate that the vehicle user is able to be informed about an update before the update is executed. The information provided may contain:  • The purpose of the update. This could include the criticality of the update and if the update is for recall, safety and/or security purposes;  • Any changes implemented by the update on vehicle functions;  • The expected time to complete execution of the update;  • Any vehicle functionalities which may not be available during the execution of the update;  • Any instructions that may help the vehicle user safely execute the update;  • In case of updates with a similar content one information may cover a group | **Observations**: OTA is mostly not implemented in the OEMs. Where implemented, this requirement seems to be met. The information to the user are mostly displayed after the update is being installed, and not before |
| **Recommendations**: Make it clear if the information for the user needs to be displayed before the start of the installation. |
| **Objective**: Check that the indicated information is made available to the user |
| 7.2.2.3 | In the situation where the execution of an update whilst driving may not be safe, the vehicle manufacturer shall demonstrate how they will:  • Ensure the vehicle cannot be driven during the execution of the update;  • Ensure that the driver is not able to use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update. | **Observations**: OTA is mostly not implemented in the OEMs. Where implemented, this requirement seems to be met. |
| **Recommendations**: |
| **Objective**: Check which functionality is blocked during OTA installations, and assess if any critical functionality is still allowed |
| 7.2.2.4. | After the execution of an update the vehicle manufacturer shall demonstrate how the following will be implemented:  • The vehicle user is able to be informed of the success (or failure) of the update;  • The vehicle user is able to be informed about the changes implemented and any related updates to the user manual (if applicable). | **Observations**: OTA is mostly not implemented in the OEMs. Where implemented, this requirement seems to be met. |
| **Recommendations**: |
| **Objective**: Check if the mentioned criteria are in place on the vehicle |

# Feedback to the Task Force



## General Feedback

* + 1. **Depth of evaluation:** There is no clarity on the depth of information to be provided to technical services during the document review and onsite assessment phases. Should Technical Services perform a deep dive into the details of the implementation in order to confirm that it is correct. In case a deep dive is required, this will take considerable time and effort. Or is a high level overview sufficient? If yes, what purpose does that serve? Example, in case the OEM claims that they implement secure pairing during software updates. Is this level sufficient for the technical services, or should they evaluate and confirm the same with additional details on the technical aspects of these implemented controls (e.g. what pairing mechanisms, which keys, which algorithms and sizes, uniqueness, etc.)? Is yes, is the manufacturer interested in sharing these technical details to the technical service? This mandates for transparency and trust. But how can that be ensured between manufacturer and technical service.
    2. **Unclear scope for assessment:** Special attention during the assessments is required for ensuring alignment on the items within the scope of the regulation. For example: Manufacturer’s backend may or may not be covered in the CSMS. The inclusion of backend is subjective based on the risk assessment. Hence, a special attention or focus is required for unclear scoped items.
    3. **Documentation clarity:** Manufacturers lack clarity in the documentation to be provided before the assessments to comply with the regulation. For example, a process documentation needs to be in place is not considered sufficiently clear to conclude what documents need to be made available and audited.
    4. **Necessity of RXSWIN:** Are alternative implementations of RXSWIN acceptable? If not, there needs to be clarity on the mandatory nature of the RXSWIN. Currently, there is no singular requirement mentioning that “RXSWIN is mandatory and needs to be implemented by the manufacturer”. Majority of manufacturers under the test phase with RDW questioned the need of RXSWIN considering the fact that technical solutions for maintaining configuration management were already in place. Moreover, with some manufacturers using one global software version(per vehicle) for any kind of update brings back to the table on what additional necessity does the RXSWIN serve. If the manufacturer is able to demonstrate comparable solutions to RXSWIN, which performs all the functions of the RXSWIN, can this solution be considered valid and sufficient? Also, RXSWIN related infrastructural implementations needs to be started at the manufacturers end at the earliest. The supporting backend implementation needs considerable lead time.
    5. **Revisiting the scope:** Some manufacturers face a market specific situation, in which they need to provide open, standardized interfaces in order to allow the vehicles to add additional trailers. The EOBD-port, FMS-interfaced and ISO7638-2(brake interface for vehicles with towing systems, trailers or other external connected system) are open interfaces. Especially in the case of FMS-interfaces (Fleet Management System), third party equipment can be of additional risk*(also to a certain extend applies for OBD-dongles)*.In this case, security is not enforced on the interface, which could lead to some security risks which have to be accepted by the manufacturer. Enforcing security would require the manufacturers of external systems to ensure additional security controls for handling risks, which is expected to be a big impact and result in a considerable delays and difficulties for implementation.
    6. **Reporting of Assessments:** Thelevel of information to be included in the final report post assessments is not clear. Some manufacturers prefer the final reports to have a minimalistic format to be delivered to the authority. For example: Only if the requirement is complied or not. While approval authorities would like to have a report from technical service with complete assessment background as well as TS’s standpoint on the approval. Then Approval authority can make its own decision/judgement based on the report. Therefore, this aspect has to be clarified. This has overlap with the confidentiality concern of the manufacturer since proprietary information goes outside the manufacturer organization. So, the overall question is if TS needs to provide a certificate or a detailed report to approval authority? Is presence of approval authority during type approval assessments prohibited?
    7. **Usage of attacker profiles:** Attacker profiles can be considered as an input to provide additional clarity for the risk assessment process. This can help in prioritizing the attack sources and in turn perform better risk assessment. During the test phase assessment process, a few manufacturers demonstrated their process on considering attacker profiles for their risk assessment process, and this can be considered as a future work for the task force group. A uniform list of attacker profiles can be identified as a reference similar to Annex B, however this list need not be exhaustive. In addition, a ranking methodology (based on business case, long term vs short term effect etc.) can be applied to distinguish between attacker profiles and to identify which attackers profiles needs to considered with a higher severity level. For e.g., a rogue attacker who has obtained root access to compromise vehicle systems against an academic attacker performing a cybersecurity research on attack vectors in vehicles. The usage of attacker profilers can also act as an input for cybersecurity policy making within contracting parties.

## Enforcement of the Regulation

* + 1. **Vehicles/vehicle systems developed before regulation enforcement:** The products designed and developed by the manufacturers before the regulation coming into force poses the risk of non-compliance. The products which were already developed or in start-of-production(SOP) through the manufacturers management systems *(Cybersecurity and Software Updates)* are not necessarily in alignment with the regulation requirements. However, the manufacturers planned deployment of their current portfolio of vehicles may continue for a longer period even after introduction of the regulation. This may result in complexities of type approval as well as the extensions. This should be considered in a sensible way by the Task Force. A possible solution could be to provide additional exemption for vehicles types with only limited vulnerability/ threat analysis.
    2. **Certificate update without RXSWIN:** The taskforce should consider the possibility to update a certificate without a RXSWIN to a certificate with a RXSWIN. In other words, for the vehicles which were produced and approved before the software update regulation, updates may no longer be formally possible once the regulation comes into force.
    3. **Exception Process:** There should be a better description of the exception process for updating software for critical risks without checking the Type-Approval relevance and without waiting for an Approval if it relevant to the type approval. This process may be supported by a temporary Type Approval or a statement from the Type Approval Authority to give a legal status to the manufacturer to update and start the TA process later within a fixed time frame.
    4. **Type approval extension overhead:** The current regulations and interpretations have to be suited also for manufacturers who operate on the basis of regular/frequent updates(like consumer device update/Agile model). The current regulatory workflow (like submitting documentation, waiting for approval, etc.) for every type approval relevant software release, has the risk of compromising velocity and agility to have continuous security and safety improvements. Hence, the workflow has to be adapted to support faster deployment of updates and more independence to manufacturers on the type approval related activities. However, the liability of such actions needs to be remain at the manufacturers’ end of informing within a specified time frame.
    5. **Objective Requirements:** There is a lack of objective behind each requirement and a corresponding defined framework for evaluation of each objective. The cybersecurity regulation specifically is contributing towards a lot of abstraction. An objective behind each requirement is necessary in order to mandate the technical services to evaluate towards that objective. This will also assist the technical services in maintaining uniformity in the assessments. There is a high chance of subjectivity in the assessments currently depending on the experience and expertise of the TS. A framework towards evaluation necessitates the objective evaluation per regulatory requirements. The NIS directive and corresponding implementation by individual country based national cybersecurity centers provides a good basis for such assessments.
    6. **Clear Instructions for initial setup and preparedness:** The regulation is particularly broad in terms of the scope, both horizontally (in terms of covered aspects) and vertically(in depth). Manufacturers have mature processes for general risk management that can be re-used for cybersecurity. Corporate IT usually has experience with the subjective nature of the CS-regulation. However, Engineering/Development likes to have clear and objective requirements for easier implementation (in line with existing regulations).
    7. **Execution of Audit:** Many manufacturers have immense difficulties with sharing documentation with technical services or approval authorities before the audit owing to manufacturer’s policy of confidentiality. In such cases, the audit phase should take into account the need for additional timeframes in order to cover both the document review and the actual audit activities. Also, Certain manufacturers would like their documents to be held secure in their own premises and not shared outside under any circumstances.

## Technical Services and Qualification

* + 1. **Competence:** Determining the technical services ability*(resources, regulation know how, standards etc.)* to perform assessments according to the regulation requirements, objectives behind each requirement and methodology of evaluation to be employed. Determining the technical services’ technical expertise for the types of management systems(Processes) and vehicle types(Products) that are within the scope of the regulation.
    2. **Confidentiality:** The cyber security assessment emphasizes an evaluation of internal cybersecurity processes for development, production and post production(monitoring and response to threats) as applied to a vehicle type. The review of the management systems is part of the evaluation carried out by approval authority or technical services. However, there is a strong need to describe the depth of evaluation across the scope of the regulation*(which deals with highly confidential design and development processes and solutions of manufacturers).* There are inherent conflicts of interests with the technical services, who simultaneously (a) have the authority to request confidential information about the product design and processes of manufacturers that they evaluate, and (b) offer consulting services to the direct competitors of those same manufacturers. So, strict confidentiality requirements needs to be in place in order to provide an absolute conducive environment to build trust and share only necessary information required for determining the objectives of the audit. For example: Sharing source code or related information is not necessitated by any requirements in the regulation and technical services should not use its position to request for code and related information for evaluation.
    3. **Impartiality:** Ensuring the technical services’ impartiality and independence of the auditors. They must provide evidence and commitments as well to ensure that the evaluations are performed in an independent and impartial manner. The technical services cannot be influenced to change the results of the evaluation. The technical services evaluations should not lead to a conflict of interest with the manufacturer, supplier or service provider of the vehicle. The compatibility of the technical service legal structure and organization to the regulatory goals and objectives.
    4. **Liability:** Liability is a serious subject in the collaboration between technical services and manufacturers for performing the assessments. Remuneration for the technical services for every assessment is comparatively low against the liability clauses introduced by manufacturer in the non-disclosure agreements. So, there is not enough drive to bring more cybersecurity technical services into the automotive market.