NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **UN Regulation No. 155 - Cyber security and cyber security management system**
Focal Document URL: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-un-155-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3	Application for approval	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.1	Application for approval	The application for approval of a vehicle type with regard to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
3.2	Application for approval	It shall be accompanied by the undermentioned documents in triplicate, and by the following particulars:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
3.2.1	Application for approval	A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
3.2.2	Application for approval	In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
3.2.3	Application for approval	The Certificate of Compliance for CSMS according to paragraph 6 of this Regulation.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
3.3	Application for approval	Documentation shall be made available in two parts:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
3.3(a)	Application for approval	The formal documentation package for the approval, containing the material specified in Annex 1 which shall be supplied to the Approval Authority or its Technical Service at the time of submission of the type approval application. This documentation package shall be used by the Approval Authority or its Technical Service as the basic reference for the approval process. The Approval Authority or its Technical Service shall ensure that this documentation package remains available for at least 10 years counted from the time when production of the vehicle type is definitively discontinued.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
3.3(b)	Application for approval	Additional material relevant to the requirements of this regulation may be retained by the manufacturer, but made open for inspection at the time of type approval. The manufacturer shall ensure that any material made open for inspection at the time of type approval remains available for at least a period of 10 years counted from the time when production of the vehicle type is definitively discontinued.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
4	Marking	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1	Marking	There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation an international approval mark consisting of:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
4.1.1	Marking	A circle surrounding the Letter "E" followed by the distinguishing number of the country which has granted approval.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
4.1.2	Marking	The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle described in paragraph 4.1.1. above.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
4.2	Marking	If the vehicle conforms to a vehicle type approved under one or more other Regulations annexed to the Agreement in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.1.1. above need not be repeated; in this case the Regulation and approval numbers and the additional symbols of all the Regulations under which approval has been granted in the country which has granted approval under this Regulation shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.1.1. above.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
4.3	Marking	The approval mark shall be clearly legible and shall be indelible.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
4.4	Marking	The approval mark shall be placed on or close to the vehicle data plate affixed by the Manufacturer.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
4.5	Marking	Annex 3 to this Regulation gives examples of the arrangements of the approval mark.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5	Approval	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1	Approval	Approval Authorities shall grant, as appropriate, type approval with regard to cyber security, only to such vehicle types that satisfy the requirements of this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.1	Approval	The Approval Authority or the Technical Service shall verify by means of document checks that the vehicle manufacturer has taken the necessary measures relevant for the vehicle type to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.1(a)	Approval	Collect and verify the information required under this Regulation through the supply chain so as to demonstrate that supplier-related risks are identified and are managed;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.1(b)	Approval	Document risks assessment (conducted during development phase or retrospectively), test results and mitigations applied to the vehicle type, including design information supporting the risk assessment;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.1(c)	Approval	Implement appropriate cyber security measures in the design of the vehicle type;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.1(d)	Approval	Detect and respond to possible cyber security attacks;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.1(e)	Approval	Log data to support the detection of cyber-attacks and provide data forensic capability to enable analysis of attempted or successful cyberattacks.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.1.2	Approval	The Approval Authority or the Technical Service shall verify by testing of a vehicle of the vehicle type that the vehicle manufacturer has implemented the cyber security measures they have documented. Tests shall be performed by the Approval Authority or the Technical Service itself or in collaboration with the vehicle manufacturer by sampling. Sampling shall be focused but not limited to risks that are assessed as high during the risk assessment.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.3	Approval	The Approval Authority or Technical Service shall refuse to grant the type approval with regard to cyber security where the vehicle manufacturer has not fulfilled one or more of the requirements referred to in paragraph 7.3., notably:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.3(a)	Approval	The vehicle manufacturer did not perform the exhaustive risk assessment referred to in paragraph 7.3.3.; including where the manufacturer did not consider all the risks related to threats referred to in Annex 5, Part A;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.3(b)	Approval	The vehicle manufacturer did not protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment or proportionate mitigations were not implemented as required by paragraph 7.;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.3(c)	Approval	The vehicle manufacturer did not put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.3(d)	Approval	The vehicle manufacturer did not perform, prior to the approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.4	Approval	The assessing Approval Authority shall also refuse to grant the type approval with regard to cyber security where the Approval Authority or Technical Service has not received sufficient information from the vehicle manufacturer to assess the cyber security of the vehicle type.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.2	Approval	Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Regulation shall be communicated to the Parties to the 1958 Agreement which apply this Regulation, by means of a form conforming to the model in Annex 2 to this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3	Approval	Approval Authorities shall not grant any type approval without verifying that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.1	Approval	The Approval Authority and its Technical Services shall ensure, in addition to the criteria laid down in Schedule 2 of the 1958 Agreement that they have:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.1(a)	Approval	Competent personnel with appropriate cyber security skills and specific automotive risk assessments knowledge;1	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.1(b)	Approval	Implemented procedures for the uniform evaluation according to this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.2	Approval	Each Contracting Party applying this Regulation shall notify and inform by its Approval Authority other Approval Authorities of the Contracting Parties applying this UN Regulation about the method and criteria taken as a basis by the notifying Authority to assess the appropriateness of the measures taken in accordance with this regulation and in particular with paragraphs 5.1., 7.2. and 7.3. This information shall be shared (a) only before granting an approval according to this Regulation for the first time and (b) each time the method or criteria for assessment is updated. This information is intended to be shared for the purposes of collection and analysis of the best practices and in view of ensuring the convergent application of this Regulation by all Approval Authorities applying this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.3	Approval	The information referred to in paragraph 5.3.2 shall be uploaded in English language to the secure internet database "DETA",2 established by the United Nations Economic Commission for Europe, in due time and no later than 14 days before an approval is granted for the first time under the methods and criteria of assessment concerned. The information shall be sufficient to understand what minimum performance levels the Approval Authority adopted for each specific requirement referred to in paragraph 5.3.2 as well as the processes and measures it applies to verify that these minimum performance levels are met.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.4	Approval	Approval Authorities receiving the information referred to in paragraph 5.3.2 may submit comments to the notifying Approval Authority by uploading them to DETA within 14 days after the day of notification.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.5	Approval	If it is not possible for the granting Approval Authority to take into account the comments received in accordance with paragraph 5.3.4., the Approval Authorities having sent comments and the granting Approval Authority shall seek further clarification in accordance with Schedule 6 to the 1958 Agreement. The relevant subsidiary Working Party4 of the World Forum for Harmonization of Vehicle Regulations (WP.29) for this Regulation shall agree on a common interpretation of methods and criteria of assessment. 5 That common interpretation shall be implemented and all Approval Authorities shall issue type approvals under this Regulation accordingly.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.6	Approval	Each Approval Authority granting a type approval pursuant to this Regulation shall notify other Approval Authorities of the approval granted. The type approval together with the supplementing documentation shall be uploaded in English language by the Approval Authority within 14 days after the day of granting the approval to DETA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.7	Approval	The Contracting Parties may study the approvals granted based on the information uploaded according to paragraph 5.3.6. In case of any diverging views between Contracting Parties this shall be settled in accordance with Article 10 and Schedule 6 of the 1958 Agreement. The Contracting Parties shall also inform the relevant subsidiary Working Party of the World Forum for Harmonization of Vehicle Regulations (WP.29) of the diverging interpretations within the meaning of Schedule 6 to the 1958 Agreement. The relevant Working Party shall support the settlement of the diverging views and may consult with WP.29 on this if needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.4	Approval	For the purpose of paragraph 7.2. of this Regulation, the manufacturer shall ensure that the cyber security aspects covered by this Regulation are implemented.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
6	Certificate of Compliance for Cyber Security Management System	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.1	Certificate of Compliance for Cyber Security Management System	Contracting Parties shall appoint an Approval Authority to carry out the assessment of the manufacturer and to issue a Certificate of Compliance for CSMS.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.2	Certificate of Compliance for Cyber Security Management System	An application for a Certificate of Compliance for Cyber Security Management System shall be submitted by the vehicle manufacturer or by their duly accredited representative.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.3	Certificate of Compliance for Cyber Security Management System	It shall be accompanied by the undermentioned documents in triplicate, and by the following particular:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.3.1	Certificate of Compliance for Cyber Security Management System	Documents describing the Cyber Security Management System.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.3.2	Certificate of Compliance for Cyber Security Management System	A signed declaration using the model as defined in Appendix 1 to Annex 1.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.4	Certificate of Compliance for Cyber Security Management System	In the context of the assessment, the manufacturer shall declare using the model as defined in Appendix 1 to Annex 1 and demonstrate to the satisfaction of the Approval Authority or its Technical Service that they have the necessary processes to comply with all the requirements for cyber security according to this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.5	Certificate of Compliance for Cyber Security Management System	When this assessment has been satisfactorily completed and in receipt of a signed declaration from the manufacturer according to the model as defined in Appendix 1 to Annex 1, a certificate named Certificate of Compliance for CSMS as described in Annex 4 to this Regulation (hereinafter the Certificate of Compliance for CSMS) shall be granted to the manufacturer.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.6	Certificate of Compliance for Cyber Security Management System	The Approval Authority or its Technical Service shall use the model set out in Annex 4 to this Regulation for the Certificate of Compliance for CSMS.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.7	Certificate of Compliance for Cyber Security Management System	The Certificate of Compliance for CSMS shall remain valid for a maximum of three years from the date of deliverance of the certificate unless it is withdrawn.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.8	Certificate of Compliance for Cyber Security Management System	The Approval Authority which has granted the Certificate of Compliance for CSMS may at any time verify that the requirements for it continue to be met. The Approval Authority shall withdraw the Certificate of Compliance for CSMS if the requirements laid down in this Regulation are no longer met.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.9	Certificate of Compliance for Cyber Security Management System	The manufacturer shall inform the Approval Authority or its Technical Service of any change that will affect the relevance of the Certificate of Compliance for CSMS. After consultation with the manufacturer, the Approval Authority or its Technical Service shall decide whether new checks are necessary.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6.10	Certificate of Compliance for Cyber Security Management System	In due time, permitting the Approval Authority to complete its assessment before the end of the period of validity of the Certificate of Compliance for CSMS, the manufacturer shall apply for a new or for the extension of the existing Certificate of Compliance for CSMS. The Approval Authority shall, subject to a positive assessment, issue a new Certificate of Compliance for CSMS or extend its validity for a further period of three years. The Approval Authority shall verify that the CSMS continue to comply with the requirements of this Regulation. The Approval Authority shall issue a new certificate in cases where changes have been brought to the attention of the Approval Authority or its Technical Service and the changes have been positively reassessed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.11	Certificate of Compliance for Cyber Security Management System	The expiry or withdrawal of the manufacturer's Certificate of Compliance for CSMS shall be considered, with regard to the vehicle types to which the CSMS concerned was relevant, as modification of approval, as referred to in paragraph 8, which may include the withdrawal of the approval if the conditions for granting the approval are not met anymore.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7	Specifications	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.1	Specifications	General specifications	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.1.1	Specifications	The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
7.2	Specifications	Requirements for the Cyber Security Management System	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.2.1	Specifications	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.2.2	Specifications	The Cyber Security Management System shall cover the following aspects:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.2.2.1	Specifications	The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases:	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7.2.2.1(a)	Specifications	Development phase;	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
7.2.2.1(b)	Specifications	Production phase;	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
7.2.2.1(c)	Specifications	Post-production phase.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
7.2.2.2	Specifications	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:	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7.2.2.2(a)	Specifications	The processes used within the manufacturer's organization to manage cyber security;	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
7.2.2.2(b)	Specifications	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;	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
7.2.2.2(b)	Specifications	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;	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:(1) Assumptions affecting risk assessments, risk response and risk monitoring;(2) Constraints affecting risk assessments, risk response and risk monitoring;(3) The organizational risk tolerance; and(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
7.2.2.2(b)	Specifications	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;	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
7.2.2.2(b)	Specifications	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;	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
7.2.2.2(b)	Specifications	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;	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
7.2.2.2(b)	Specifications	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;	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
7.2.2.2(b)	Specifications	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;	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	8	
7.2.2.2(c)	Specifications	The processes used for the assessment, categorization and treatment of the risks identified;	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	8	
7.2.2.2(c)	Specifications	The processes used for the assessment, categorization and treatment of the risks identified;	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
7.2.2.2(c)	Specifications	The processes used for the assessment, categorization and treatment of the risks identified;	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
7.2.2.2(d)	Specifications	The processes in place to verify that the risks identified are appropriately managed;	Functional	Subset Of	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;	10	
7.2.2.2(d)	Specifications	The processes in place to verify that the risks identified are appropriately managed;	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
7.2.2.2(e)	Specifications	The processes used for testing the cyber security of a vehicle type;	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	8	
7.2.2.2(e)	Specifications	The processes used for testing the cyber security of a vehicle type;	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	
7.2.2.2(f)	Specifications	The processes used for ensuring that the risk assessment is kept current;	Functional	Subset Of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.2.2.2(f)	Specifications	The processes used for ensuring that the risk assessment is kept current;	Functional	Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	8	
7.2.2.2(g)	Specifications	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.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
7.2.2.2(g)	Specifications	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.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
7.2.2.2(g)	Specifications	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.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	8	
7.2.2.2(g)	Specifications	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.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
7.2.2.2(g)	Specifications	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.	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
7.2.2.2(g)	Specifications	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.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
7.2.2.2(g)	Specifications	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.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	8	
7.2.2.2(h)	Specifications	The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
7.2.2.2(h)	Specifications	The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IOC).	8	
7.2.2.2(h)	Specifications	The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
7.2.2.2(h)	Specifications	The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7.2.2.3	Specifications	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.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
7.2.2.3	Specifications	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.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related:(1) Assessments;(2) Audits; and/or(3) Incidents.	8	
7.2.2.3	Specifications	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.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	3	
7.2.2.3	Specifications	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.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	8	
7.2.2.3	Specifications	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.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
7.2.2.3	Specifications	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.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	8	
7.2.2.3	Specifications	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.	Functional	Intersects With	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	3	
7.2.2.3	Specifications	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.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	8	
7.2.2.4	Specifications	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:	Functional	Intersects With	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	8	
7.2.2.4(a)	Specifications	Include vehicles after first registration in the monitoring;	Functional	Intersects With	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	8	
7.2.2.4(b)	Specifications	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.	Functional	Intersects With	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	8	
7.2.2.5	Specifications	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.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
7.2.2.5	Specifications	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.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
7.2.2.5	Specifications	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.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
7.2.2.5	Specifications	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.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
7.2.2.5	Specifications	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.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
7.2.2.5	Specifications	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.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7.2.2.5	Specifications	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.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
7.2.2.5	Specifications	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.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
7.3	Specifications	Requirements for vehicle types	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.3.1	Specifications	The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved. However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.2	Specifications	The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.3	Specifications	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.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.4	Specifications	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.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.5	Specifications	The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.6	Specifications	The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.7	Specifications	The vehicle manufacturer shall implement measures for the vehicle type to:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.7(a)	Specifications	Detect and prevent cyber-attacks against vehicles of the vehicle type;	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.7(b)	Specifications	Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.7(c)	Specifications	Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.3.8	Specifications	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.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.4	Specifications	Reporting provisions	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.4.1	Specifications	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.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
7.4.2	Specifications	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.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
8	Modification and extension of the vehicle type	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.1	Modification and extension of the vehicle type	Every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in this Regulation shall be notified to the approval authority which approved the vehicle type. The Approval Authority may then either:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
8.1.1	Modification and extension of the vehicle type	Consider that the modifications made still comply with the requirements and documentation of existing type approval; or	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
8.1.2	Modification and extension of the vehicle type	Proceed to necessary complementary assessment pursuant to paragraph 5, and require, where relevant, a further test report from the Technical Service responsible for conducting the tests.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
8.1.3	Modification and extension of the vehicle type	Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex 2 to this Regulation. The Approval Authority issuing the extension of approval shall assign a series number for such an extension and inform there of the other Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 2 to this Regulation.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
9	Conformity of production	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.1	Conformity of production	The Conformity of Production Procedures shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) with the following requirements:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
9.1.1	Conformity of production	The holder of the approval shall ensure that results of the conformity of production tests are recorded and that the annexed documents remain available for a period determined in agreement with the Approval Authority or its Technical Service. This period shall not exceed 10 years counted from the time when production is definitively discontinued;	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
9.1.2	Conformity of production	The Approval Authority which has granted type approval may at any time verify the conformity control methods applied in each production facility. The normal frequency of these verifications shall be once every three years.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
10	Penalties for non-conformity of production	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.1	Penalties for non-conformity of production	The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in this Regulation are not complied with or if sample vehicles fail to comply with the requirements of this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.2	Penalties for non-conformity of production	If an Approval Authority withdraws an approval it has previously granted, it shall forthwith so notify the Contracting Parties applying this Regulation, by means of a communication form conforming to the model in Annex 2 to this Regulation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11	Production definitively discontinued	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11.1	Production definitively discontinued	If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the authority which granted the approval. Upon receiving the relevant communication that authority shall inform thereof the other Contracting Parties to the Agreement applying this Regulation by means of a copy of the approval form bearing at the end, in large letters, the signed and dated annotation "PRODUCTION DISCONTINUED".	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
12	Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.1	Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities	The Contracting Parties to the Agreement which apply this Regulation shall communicate to the United Nations Secretariat the names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval, issued in other countries, are to be sent.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control