SmartSuite

Framework / Cybersecurity / Other

UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems

UN Regulation No. 155 (UN R155) makes vehicle type approval conditional on a certified Cyber Security Management System and a documented risk assessment and mitigations per vehicle type.



What it is

UN Regulation No. 155, Uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems (UN R155), is the UNECE regulation annexed to the 1958 Agreement that makes the type approval of a vehicle type conditional on a certified Cyber Security Management System (CSMS) at the manufacturer and on a documented risk assessment, mitigations and testing for that vehicle type. It binds vehicle manufacturers seeking type approval in the Contracting Parties that apply it, among them the European Union and its member states, the United Kingdom, Japan, the Republic of Korea, Australia and South Africa; the original text entered into force on January 22, 2021.

At a glance

PUBLISHER
UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) and the Administrative Committee of the 1958 Agreement (AC.1); drafted by GRVA

TYPE
Regulation

VERSION
Original text (00 series, ECE/TRANS/WP.29/2020/79) with Supplement 1 (in force October 8, 2022), Supplement 2 (January 5, 2024) and Supplement 3 (January 10, 2025)

EFFECTIVE
January 22, 2021 (original text); Supplement 3 in force January 10, 2025

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Contracting Parties to the 1958 Agreement that apply the Regulation (EU and member states, UK, Japan, Republic of Korea, Australia, South Africa and others)

INDUSTRY
Automotive

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160

Why it matters

- **Approval depends on it** Paragraph 5.1.3 requires the Approval Authority to refuse type approval where the manufacturer has not performed the exhaustive risk assessment of 7.3.3, has not implemented proportionate mitigations or has not tested them before approval.
- **One certificate, many vehicle types** The Certificate of Compliance for CSMS (paragraph 6, Annex 4) covers the manufacturer's processes and is valid for a maximum of three years (6.7); each vehicle type approval then references its number (Annex 1, item 9.3).
- **A shared threat catalog** Annex 5, Part A lists the threats and attack methods every risk assessment must consider (7.2.2.2(b), 7.3.3), grouped from back-end servers to external connectivity and vehicle data and code.
- **Lifecycle coverage** The CSMS must apply to the development, production and post-production phases (7.2.2.1), with post-production defined as lasting until no vehicles of the type remain in operation (2.7).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports UNECE R155

CSMS Process Library (7.2.2.2)

Load the eight process areas (a) to (h), the lifecycle phases of 7.2.2.1 and the supplier dependency rule of 7.2.2.5 as controls with owners, status and the evidence the Approval Authority assesses.

Vehicle Type Risk Assessment (7.3.3, Annex 5 Part A)

Record the critical elements, the seven Annex 5 threat groups and other relevant threats per vehicle type, with the attack impacts of Annex 5 paragraph 4 and the risk categorization of 7.2.2.2(c).

Mitigation Traceability (7.3.4, Annex 5 Parts B and C)

Link each Annex 5 mitigation reference or justified alternative to the risk it treats, the design element it protects and the pre-approval test of 7.3.6 that verified it.

Monitoring and Response Log (7.2.2.4, 7.3.7)

Track detected threats, vulnerabilities and attacks on vehicles in the field, the response decision and the timeframe of 7.2.2.3, and the forensic data provided under 7.2.2.2(h).

Supplier Dependencies (7.2.2.5, 7.3.2, 5.1.1(a))

Hold each contracted supplier's cybersecurity obligations, the information collected through the supply chain and the open risks per vehicle type.

Certificate and Reporting Calendar (6.7, 7.4.1, 9.1.2)

Schedule the three-year CSMS certificate renewal, the annual report to the Approval Authority, conformity of production verifications and the ten-year documentation retention of 3.3.

Common framework mappings

GDPR | ISO 27001:2022 | ISO/SAE 21434 | MITRE ATT&CK

Official resources

UN Regulation No. 155, adopted text (ECE/TRANS/WP.29/2020/79)

The text of the Regulation on cyber security and cyber security management systems as adopted by WP.29 in June 2020.

documents.un.org/doc/undoc/gen/g20/079/73/pdf/g2007973.pdf

Supplement 3 to UN Regulation No. 155 (ECE/TRANS/WP.29/2024/55)

The June 2024 supplement that extends the scope to Category L vehicles and amends paragraph 7.3.1.

documents.un.org/doc/undoc/gen/g24/063/12/pdf/g2406312.pdf

Interpretation document for UN Regulation No. 155 (ECE/TRANS/WP.29/2021/59)

The WP.29 interpretation document that explains how the CSMS and vehicle-type requirements are assessed.

documents.un.org/doc/undoc/gen/g20/353/49/pdf/g2035349.pdf

Status of the 1958 Agreement (ECE/TRANS/WP.29/343/Rev.33)

The 2025 status document listing the Contracting Parties and the UN Regulations annexed to the 1958 Agreement, including No. 155.

documents.un.org/doc/undoc/gen/g25/030/18/pdf/g2503018.pdf

Frequently asked questions

Which vehicles does UN Regulation No. 155 apply to?

Since Supplement 3 entered into force on January 10, 2025, paragraph 1.1 applies the Regulation to vehicles of Categories L, M, N and O with regard to cyber security, if fitted with at least one electronic control unit. As adopted in 2020 it covered Categories M and N, Category O with at least one electronic control unit, and L6 and L7 vehicles with automated driving from level 3 (former paragraph 1.2). For Category L, type approvals first issued before July 1, 2029 may rely on the transitional wording of paragraph 7.3.1.

What is a Cyber Security Management System under UN R155, and how long is its certificate valid?

Paragraph 2.3 defines the CSMS as a systematic risk-based approach defining organizational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks. The Approval Authority assesses the manufacturer and issues a Certificate of Compliance for CSMS in the form of Annex 4 (6.1 to 6.6). The certificate is valid for a maximum of three years unless withdrawn (6.7), can be verified at any time (6.8) and is renewed or extended for a further three years after a positive assessment (6.10).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What must the CSMS cover?

Paragraph 7.2.2.1 requires the CSMS to apply to the development, production and post-production phases. Paragraph 7.2.2.2 lists the processes: managing cyber security in the organization, identifying risks to vehicle types including the Annex 5 Part A threats, assessing, categorizing and treating risks, verifying they are managed, testing the cyber security of a vehicle type, keeping the risk assessment current, monitoring, detecting and responding to attacks, threats and vulnerabilities, and providing data to analyze attacks. Mitigation must follow within a reasonable timeframe (7.2.2.3), monitoring must be continual and include vehicles after first registration (7.2.2.4), and supplier dependencies must be managed (7.2.2.5).

What does a manufacturer have to show for each vehicle type?

Paragraph 7.3 requires a valid CSMS certificate (7.3.1), management of supplier-related risks (7.3.2), identification of the critical elements and an exhaustive risk assessment that considers the Annex 5 Part A threats, the elements' interactions and external systems (7.3.3), proportionate mitigations including the relevant Annex 5 Part B and C measures or justified alternatives (7.3.4), secured dedicated environments for aftermarket software (7.3.5), appropriate and sufficient testing before approval (7.3.6), measures for detection, monitoring and forensics (7.3.7) and cryptographic modules in line with consensus standards (7.3.8). The Authority checks the documents and tests a sample vehicle (5.1.1, 5.1.2) and must refuse approval if 7.3 is not met (5.1.3).

When did UN R155 and its supplements enter into force?

WP.29 adopted the Regulation at its 181st session in June 2020 (report ECE/TRANS/WP.29/1153, paragraph 49) and the original text entered into force on January 22, 2021. The status document ECE/TRANS/WP.29/343/Rev.33/Add.2 records Supplement 1 in force on October 8, 2022 (transitional wording for approvals first issued before July 1, 2024), Supplement 2 on January 5, 2024 (spoofing and Sybil attacks in Annex 5) and Supplement 3 on January 10, 2025 (scope extended to Category L). Ongoing obligations such as the annual report under 7.4.1 continue for as long as the vehicle type is in production or on the road.

License included / downloadable: Yes UN Regulation No. 155 is a United Nations document: the adopted text and its supplements are free on the UNECE vehicle regulations pages and, by document symbol, on documents.un.org (ECE/TRANS/WP.29/2020/79; 2022/54; 2023/70; 2024/55).

Full framework page and mappings: smartsuite.com/frameworks/un-regulation-no-155-cybersecurity-and-cybersecurity-management-system