SmartSuite

Framework / Cybersecurity / Other

UN Regulation No. 155 (R155) — Cybersecurity & CSMS

UN Regulation No. 155 mandates vehicle cybersecurity management systems to protect vehicles throughout their lifecycle.

What it is

UNECE WP.29 — Vehicle Cybersecurity Regulation (R155) is an international automotive cybersecurity regulation that requires vehicle manufacturers to implement and maintain robust cybersecurity management systems to ensure the security of vehicles throughout their lifecycle. Its primary goal is to mitigate cybersecurity risks that could impact road safety, vehicle operations, and data protection.

Published by the United Nations Economic Commission for Europe (UNECE), this regulation is mandatory for automotive manufacturers selling vehicles in markets governed by UNECE member states, including much of Europe and parts of Asia. R155 provides requirements related to risk management, secure software updates, and the protection of vehicle electronic systems from cyber threats, supporting organizations in establishing effective cybersecurity controls and compliance practices.

At a glance

PUBLISHER United Nations Economic Commission for Europe (UNECE)	TYPE Regulation	VERSION 2020
EFFECTIVE 22 January 2021	DOMAIN Cybersecurity	FAMILY Other
REGION United Nations Economic Commission for Europe (UNECE)	INDUSTRY Automotive	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://unece.org/transport/documents/2022/11/standards/un-regulation-no-155-amend1-0

Why it matters

- **Strengthen cybersecurity governance** Promote a structured, organization-wide approach to managing vehicle cybersecurity risks and enforcing security accountability across product teams.
- **Enhance regulatory alignment** Enable compliance with international requirements, supporting lawful vehicle market access and aligning automotive practices with global regulatory expectations.
- **Improve incident response readiness** Mandate development of processes for timely detection of, and effective response to, cyber threats affecting vehicle safety or operational integrity.
- **Protect sensitive vehicle data** Support robust safeguards for in-car data and critical vehicle functions, minimizing the risk of unauthorized access or data breaches.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports UNECE R155

Cybersecurity Management System (CSMS)

Organize policies, governance, and processes required for vehicle cybersecurity certification.

Vehicle Risk Assessment and TARA Tracking

Manage threat analysis and risk assessments across vehicle platforms and components.

Control Implementation and Traceability

Link cybersecurity controls to risks, systems, and lifecycle requirements.

Vehicle Vulnerability and Incident Management

Track vulnerability disclosures, incident investigations, and remediation activities affecting vehicle systems.

Supplier and Supply Chain Security Oversight

Manage supplier requirements, assurance evidence, and third-party cybersecurity risks.

Regulatory Compliance and Type Approval Reporting

Provide dashboards supporting CSMS compliance, audit readiness, and regulatory submissions.

Common framework mappings

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

Official resources

UNECE WP.29 — Vehicle Cybersecurity Regulation (R155)

Defines cybersecurity requirements for automotive manufacturers to ensure vehicle security throughout its lifecycle.

unece.org/transport/vehicle-regulations/un-regulation-no-155-cyber-security

UNECE R155 Implementation Guidance

Outlines guidance on implementing the UNECE R155 cybersecurity regulation for vehicle manufacturers.

unece.org/transport/vehicle-regulations

UNECE WP.29 Cybersecurity Management System (CSMS) Guide

Provides detailed instructions for establishing a Cybersecurity Management System under UNECE R155.

unece.org/transport/vehicle-regulations/csms-guide

UNECE R155 Regulatory Framework Overview

Describes the structure and objectives of the UNECE WP.29 Vehicle Cybersecurity Regulation.

unece.org/transport/vehicle-regulations/framework-overview

Frequently asked questions

What is UN Regulation No. 155 used for?

UN Regulation No. 155 establishes mandatory requirements for automotive cybersecurity management systems (CSMS) to ensure vehicles are protected against cyber threats throughout their lifecycle. Its primary goal is to address cybersecurity risks in the design, development, production, and post-production of vehicles.

Is compliance with UN Regulation No. 155 mandatory?

Yes, compliance with UN Regulation No. 155 is mandatory for vehicle manufacturers seeking type approval in many jurisdictions, including the European Union. Without demonstrating compliance, manufacturers cannot market new vehicle types in these regions.

What types of vehicles or components does UN Regulation No. 155 apply to?

UN Regulation No. 155 applies to passenger vehicles, light commercial vehicles, heavy-duty vehicles, and buses. It also covers electronic components and systems related to cybersecurity, throughout their supply chain.

What is a Cybersecurity Management System (CSMS) under UN Regulation No. 155?

A CSMS is a formal set of processes, policies, and procedures required by UN Regulation No. 155 to manage and mitigate cybersecurity risks throughout a vehicle's lifecycle. Key artifacts include documented risk assessments, incident response plans, and security testing evidence.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How should organizations implement UN Regulation No. 155 requirements?

Implementation involves developing and maintaining a CSMS, performing vehicle and component risk assessments, defining and applying cybersecurity controls, and preparing for incident detection and response. Organizations must also ensure traceability, accountability, and continuous improvement within their cybersecurity management processes.

How does UN Regulation No. 155 relate to other cybersecurity standards?

UN Regulation No. 155 complements existing cybersecurity standards such as ISO/SAE 21434 by embedding similar risk management principles and controls into regulatory requirements. While ISO/SAE 21434 provides technical guidance, UN R155 is legally enforced and necessary for type approval.

What ongoing compliance activities are needed for UN Regulation No. 155?

Organizations must regularly update their CSMS, conduct continuous risk monitoring, log and respond to incidents, and document all activities for audit and regulatory review. Periodic reviews and evidence-based reporting are required to demonstrate ongoing compliance for type-approved vehicles.

How would SmartSuite support UN Regulation No. 155?

SmartSuite enables organizations to manage UN Regulation No. 155 compliance by facilitating cybersecurity risk tracking, control implementation, and ongoing evidence collection. It provides tools for documentation, workflow management, audit readiness, and streamlined reporting, supporting continuous oversight and regulatory alignment.

What is UNECE WP.29 R155 used for?

UNECE WP.29 Regulation R155 is used to establish minimum cybersecurity requirements for vehicles, ensuring that manufacturers manage cyber risks throughout a vehicle's lifecycle. It provides a regulatory basis for addressing threats to vehicle systems and road safety through structured cybersecurity controls and processes.

License included / downloadable: Yes UN Regulation No. 155 is published by the UNECE/WP.29 and is publicly available on the UNECE website. License included with platform

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

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.