Automate Your Software Security Compliance

Generate submission-ready vulnerability assessments and documentation at vehicle and component levels.

RUNSAFE SECURITY

Documentation Category	ISO Clause	ISO Requirements / Example Content	RunSafe	RunSafe Capability/Notes	How This Feeds OEM R155 CSMS
Item Definition Defines the ECU/system scope, functionality, interfaces, and operating environment. Establishes cybersecurity boundaries	ISO 21434: Clause 9.3	Item/system description documented		Subject to RunSafe customers' practices	OEM demonstrates knowledge of vehicle architecture and attack surface across suppliers (R155 Annex 5 risk identification).
	ISO 21434: Clause 9.3	System boundaries clearly defined		Subject to RunSafe customers' practices	
	ISO 21434: Clause 9.3	External/internal interfaces identified		Subject to RunSafe customers' practices	
	ISO 21434: Clause 15.3	Assets identified (data, functions, credentials, etc.)	✓	Reports on all software components enumerating all NTIA minimum elements.	
	ISO 21434: Clause 9.3	Operational environment described		Subject to RunSafe customers' practices	
	ISO 21434: Clause 9.3	Assumptions and dependencies documented	✓	Automates SBOM generation, which clarifies all software components with afull dependency tree.	
TARA (Threat Analysis & Risk Assessment) Structured process to identify threats, assess risks, and determine risk treatment	ISO 21434: Clause 15.3, 15.4	Assets mapped to threat scenarios	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and potential zero days	OEM CSMS shows systematic risk assessment including supplier components (R155 risk management process).
	ISO 21434: Clause 15.4	Threat scenarios identified and documented		Subject to RunSafe customers' practices	
	ISO 21434: Clause 15.7	Attack feasibility evaluated	✓	Risk Reduction Analysis identifies memory corruption vulnerabilities and exploitability, informing attack feasibility	
	ISO 21434: Clause 15.5	Impact ratings assigned	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).	
	ISO 21434: Clause 15.7	Risk level calculated	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).	
	ISO 21434: Clause 15.9	Risk treatment decision documented		Subject to RunSafe customers' practices	
	ISO 21434: Clause 15.3-15.7, 6.4	Traceability from assets to threats/risks maintained		Subject to RunSafe customers' practices	
Cybersecurity Concept High-level security strategy defining how identified risks will be mitigated	ISO 21434: Clause 9.4	Cybersecurity goals defined		Subject to RunSafe customers' practices	OEM demonstrates risk treatment strategy across vehicle architecture and supplier mitigations (R155 Annex 5 mitigation).
	ISO 21434: Clause 9.4, 15.9	Mitigations mapped to identified risks	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RunSafe Protect makes a vulnerability non-exploitable.	
	ISO 21434: Clause 9.5	Trust boundaries identified		Subject to RunSafe customers' practices	
	ISO 21434: Clause 9.5	Security controls conceptually defined	✓	RunSafe Protect provides control that eliminates exploitation of entire classes of vulns even when a patch is not available	
	ISO 21434: Clause 9.3	Assumptions on vehicle-level protections stated		Subject to RunSafe customers' practices	
	ISO 21434: Clause 9.5, 15	Consistency with TARA demonstrated		Subject to RunSafe customers' practices	
Cybersecurity Requirements & Architecture Detailed technical security requirements and architecture implementing the concept.	ISO 21434: Clause 10.4.1	Cybersecurity requirements specified and documented		Subject to RunSafe customers' practices	OEM shows cybersecurity is engineered into components and integrated into vehicle design (R155 development controls).
	ISO 21434: Clause 10.4.1	Requirements allocated to system elements	✓	Specify vulnerability and shows mitigation at software component level using Risk Reduction Analysis tool and RunSafe Protect to mitigate vulnerabilities.	
	ISO 21434: Clause 10.4.1	Secure architecture defined		Subject to RunSafe customers' practices	
	ISO 21434: Clause 10.4.1	Authentication, authorization, and crypto addressed		Subject to RunSafe customers' practices	
	ISO 21434: Clause 10.4.1	Secure communication defined		Subject to RunSafe customers' practices	
	ISO 21434: Clause 10.4.1	Key management defined		Subject to RunSafe customers' practices	
	ISO 21434: Clause 6.4	Requirement traceability maintained	✓	RunSafe identifies the vulns so that users can triage patches	
Verification & Validation Evidence Demonstrates implementation and effectiveness of cybersecurity requirements	ISO 21434: Clause 10.4.2	Security verification plan documented		Subject to RunSafe customers' practices	OEM shows mitigations are verified and effective across suppliers (R155 validation & effectiveness evidence).
	ISO 21434: Clause 6.4	Requirements-to-test traceability present	✓	Testing, scanning and analysis is performed using Risk Reduction Analysis as well as RunSafe incorporating dozens of sources (including NVD and vendor advisors) to identify vulnerabilities associated with each component of an SBOM	
	ISO 21434: Clause 10.4.2	Security testing executed (static, dynamic, fuzzing, etc.)		Subject to RunSafe customers' practices	
	ISO 21434: Clause 11.4	Penetration testing performed (if applicable)		Subject to RunSafe customers' practices	
	ISO 21434: Clause 10.4.2, 8.5, 8.6	Identified vulnerabilities tracked and resolved	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RS Protect makes vulnerability non-exploitable.	
	ISO 21434: Clause 10.4.2, 11.4	Test results documented and approved		Subject to RunSafe customers' practices	
Residual Risk & Cybersecurity Case Justifies acceptance of remaining cybersecurity risks	ISO 21434: Clause 15.7	Residual risks identified	✓	Risk Reduction Analysis — shows which CVEs remain exploitable vs mitigated.	OEM must justify acceptable residual vehicle risk including supplier components (R155 risk acceptance).
	ISO 21434: Clause 15.9	Risk acceptance rationale documented	✓	Risk Reduction Analysis — shows which CVEs remain exploitable vs mitigated. RunSafe Protect makes vulnerability non-expliotable.	
	ISO 21434: Clause 9.3	Integration assumptions defined		Subject to RunSafe customers' practices	
	ISO 21434: Clause 10.4.1	Dependencies on OEM or other components stated		Subject to RunSafe customers' practices	
	ISO 21434: Clause 6.4	Cybersecurity assurance argument compiled		Subject to RunSafe customers' practices	
	ISO 21434: Clause 15.9	Management approval recorded		Subject to RunSafe customers' practices	
SBOM & Vulnerability Status Software component inventory and current vulnerability posture	ISO 21434: Clause 10.4.1, 12.4	SBOM generated (components and versions listed)	✓	RunSafe generates a buildtiime SBOM so it is created when firmware or software image is produced, and reports on all mandatory NTIA minimum elements	OEM demonstrates vulnerability management across lifecycle and suppliers (R155 Annex 5 vulnerability monitoring).
	ISO 21434: Clause 10.4.1	Third-party and OSS components identified	✓	RunSafe covers all software (OS, firmware, apps, libraries) with a full depedency tree.	
	ISO 21434: Clause 8.5	Known vulnerabilities assessed (CVE review)	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and potential zero days; and determines if a vuln is exploitable	
	ISO 21434: Clause 15.7	Exploitability evaluated	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RS Protect makes vulnerability non-exploitable.	
	ISO 21434: Clause 15.9, 8.6	Mitigation or patch plan documented	✓	RunSafe identifies vulns so that users can triage patches; also RunSafe confirms when a vulnerability is not exploitable	
	ISO 21434: Clause 8.6	Vulnerability tracking process defined		Subject to RunSafe customers' practices	
Post-Development Monitoring & Response Plan Defines how cybersecurity is maintained after SOP/production release	ISO 21434: Clause 8.3	Vulnerability monitoring process established	✓	Supports VEX to communicate known, specific vulnerabilities	OEM shows post-production monitoring, incident response, and supplier coordination (R155 lifecycle obligations).
	ISO 21434: Clause 13.3	PSIRT contact and workflow defined		Subject to RunSafe customers' practices	
	ISO 21434: Clause 8.5, 8.6	Vulnerability intake and triage procedure documented	✓	Incorporate RunSafe in the vulnerability investigation process. RunSafe incorporate sources to identify vulnerabilities with the SBOM, monitors for new alerts, andanalyzes exposure to CVEs and potential zero days; and determines if exploitable	
	ISO 21434: Clause 8.6	Coordinated disclosure process defined			
	ISO 21434: Clause 13.4	Update/patch strategy defined	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).	
	ISO 21434: Clause 13.3	OEM notification process defined		Subject to RunSafe customers' practices	
	ISO 21434: Clause 13	Support and maintenance period defined		Subject to RunSafe customers' practices	