Ministero delle Infrastrutture e della Mobilità Sostenibili

Dipartimento per la mobilità sostenibile

Direzione Generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione

Regolamento ONU n. 155

Prescrizioni concernenti l'omologazione dei veicoli per quanto riguarda la sicurezza cibernetica e il sistema di gestione della sicurezza cibernetica

Metodi e criteri

Versione 1.0 del 3/08/2022

SOMMARIO

1. FINALITÀ DEL DOCUMENTO

Il presente documento descrive le modalità, i metodi e i criteri utilizzati dall'Autorità di Omologazione in Italia al fine di rilasciare una omologazione per un nuovo tipo di veicoli ai sensi del Regolamento UN R155.

Nel documento sono evidenziate e separate fra loro le sezioni applicabili all'audit del Sistema di Gestione della Sicurezza Informatica (CSMS) del Costruttore, con il rilascio del relativo certificato, nonché quelle delle sezioni applicabili alla valutazione del tipo di veicolo in approvazione e alle prove ad esso applicabili.

Il presente documento è stato redatto alla luce delle interpretazioni adottate dal Forum mondiale per l'armonizzazione delle normative sui veicoli (WP.29) dell'UNECE (vedi documento ECE/TRANS/WP.29/2022/61). Il presente documento sarà rivisto in base sia alle indicazioni ricevute in ambito internazionale (UN) che in base alle esperienze maturate.

2. DEFINIZIONI

Il presente documento è redatto utilizzando le definizioni stabilite nell'ambito delle norme di omologazioni e, in particolare, a quelle stabilite nel Regolamento UN n. 155 e nell'Accordo internazionale relativo all'adozione di condizioni uniformi di omologazione ed al riconoscimento reciproco dell'omologazione degli accessori e parti di veicoli a motore firmato a Ginevra il 20 marzo 1958 (58A Rev.3).

Per quanto non definito nella richiamata normativa, si deve intendere per:

- Commissione: la Commissione incaricata, con disposizione del Direttore dell'Autorità di omologazione, per la conduzione dell'audizione finalizzata alla verifica del CSMS;
- Autorità di omologazione: la Divisione 3 della Direzione Generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione del Ministero delle infrastrutture e della mobilità sostenibili;
- Servizio Tecnico: sono gli uffici decentrati del Ministero delle infrastrutture e della mobilità sostenibili denominati Centro Superiore Ricerche e Prove Autoveicoli e Dispositivi (CSRPAD) e Centro Prove Autoveicoli (CPA) nonché il Servizio Tecnico incardinato nella Divisione 3 della Direzione Generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione;
- Posta Elettronica Certificata (PEC): è il sistema che consente di inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno, come stabilito dalla normativa nazionale.

L'Autorità di Omologazione in Italia è individuata presso il Ministero delle Infrastrutture e della Mobilità Sostenibili. I suoi riferimenti sono i seguenti:

Ministero delle Infrastrutture e della Mobilità Sostenibili
Dipartimento per la mobilità sostenibile
Direzione generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione
Divisione 3 – Disciplina tecnica dei veicoli e Autorità di omologazione (Vehicle Type Approvals)
Via Giuseppe Caraci, 36, Roma, Città Metropolitana di Roma, 00157, Lazio, Italia
Email certificata: dg.mot-div3@pec.mit.gov.it
Email: div3.dgmot@mit.gov.it
Telefono: 06/44128473 – 41

3. PROCESSI DI VALUTAZIONE DELLA CONFORMITÀ

La valutazione della conformità del CSMS nonché l'emissione della certificazione è affidata all'Autorità di omologazione.

La valutazione del tipo di veicolo in approvazione è affidata al Servizio Tecnico.

3.1 DESCRIZIONE DEL PROCESSO (Diagramma di flusso)

3.1.1 RILASCIO DEL CERTIFICATO CSMS

Il processo per la valutazione di conformità del CSMS del Costruttore prevede le seguenti fasi:

- Esame documentale;
- Preparazione dell'audit;
- Conduzione dell'audit presso il Costruttore;
- Stesura del verbale di audit (Allegato 4);
- Comunicazione dell'esito della valutazione;
- Eventuale audit aggiuntivo;
- Emissione del certificato CSMS.

Il processo è descritto nel dettaglio nel Diagramma di flusso di cui alla Figura 1.

Il certificato CSMS ha una durata di tre anni dalla data di emissione. Nel corso del periodo di validità il Costruttore sarà sottoposto ad audit di sorveglianza con periodicità almeno annuale da parte dell'Autorità di omologazione.

Alla scadenza dei tre anni di validità il certificato CSMS può essere rinnovato con la ripetizione del processo di audit completo.

Il Costruttore è tenuto a segnalare all'Autorità di omologazione, mediante PEC, ogni modifica sostanziale apportata al CSMS che abbia o meno un potenziale impatto sulla validità del certificato. L'Autorità di omologazione, valutata la documentazione presentata dal Costruttore, deciderà se ritenere che le modifiche apportate siano ancora conformi alle prescrizioni e alla documentazione dell'omologazione esistente, ovvero se procedere alla necessaria valutazione complementare per il rinnovo del CSMS dandone riscontro al Costruttore via PEC entro un tempo ragionevole di circa un mese.

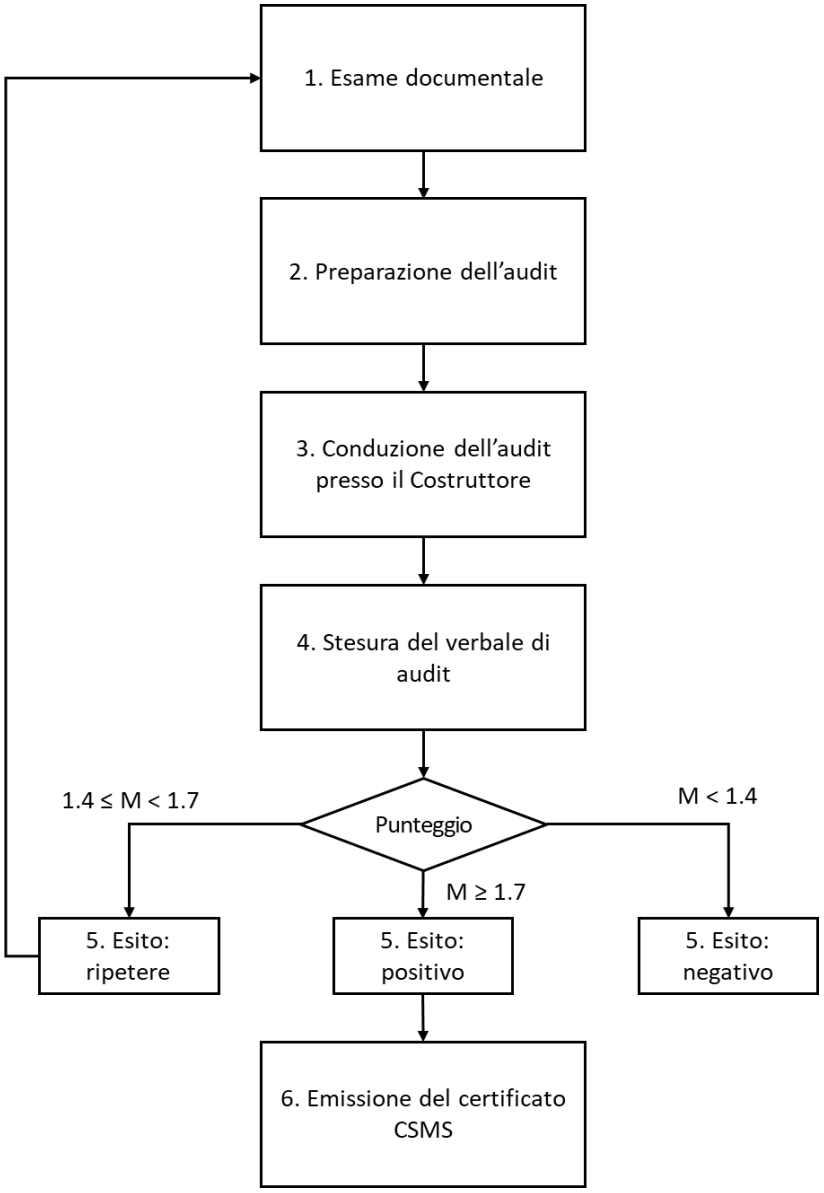


Figura 1 – Diagramma di flusso del processo di audit CSMS

Tutta la documentazione ricevuta sarà valutata sulla base di criteri generali, ad esempio, che siano controllati, utilizzati, accessibili, revisionati, ecc.

Tali informazioni verranno raccolte in un modello indicato in tabella 1:

N.	Titolo	Descrizione	Osservazioni	Valutazione

Tabella 1 – Scheda documentazione

Durante l'esecuzione dell'audit verranno registrate tutte le informazioni, non deducibili dalla documentazione, in un questionario di audit secondo il modello indicato in tabella 2:

Requisiti	Domande di verifica	Intento/Scopo della domanda	Criteri minimi di prestazioni	Migliori pratiche	Ulteriori informazioni/Contesto

Tabella 2 – Scheda audizione

3.1.2 APPROVAZIONE DEL TIPO DI VEICOLO

Il processo per l'approvazione del tipo di veicolo, ai sensi del Reg. UN R155, prevede le seguenti fasi:

- Controllo di validità del certificato CSMS del Costruttore;
- Esame documentale;
- Preparazione della visita di omologazione;
- Conduzione della visita di omologazione presso il Costruttore;
- Ripetizione di prove sul veicolo;
- Stesura del verbale di omologazione (Allegato 5);
- Comunicazione dell'esito della valutazione;
- Emissione del certificato di omologazione.

Il suddetto processo è descritto nel dettaglio nel Diagramma di flusso di cui alla Figura 2.

Il Servizio Tecnico valuta, in via preliminare, se il CSMS detenuto dal Costruttore sia da integrare o modificare o se sia sufficiente per la positiva sottoscrizione del verbale. Qualora il CSMS sia da integrare o modificare, il Servizio Tecnico sospenderà il processo segnalando la necessità di adeguamento del CSMS all'Autorità di omologazione e al costruttore.

Il Servizio Tecnico deve verificare, mediante prove su un veicolo del tipo in questione o di sistemi o sottosistemi dello stesso, che il costruttore dello stesso abbia attuato le misure di cybersicurezza da esso documentate. Le prove devono essere eseguite dal Servizio Tecnico in collaborazione con il costruttore del veicolo mediante campionamento e, di norma, con l'impiego di soggetti terzi rispetto al costruttore. Il campionamento deve essere incentrato, a titolo non esaustivo, sui rischi che sono giudicati elevati in fase di valutazione del rischio.

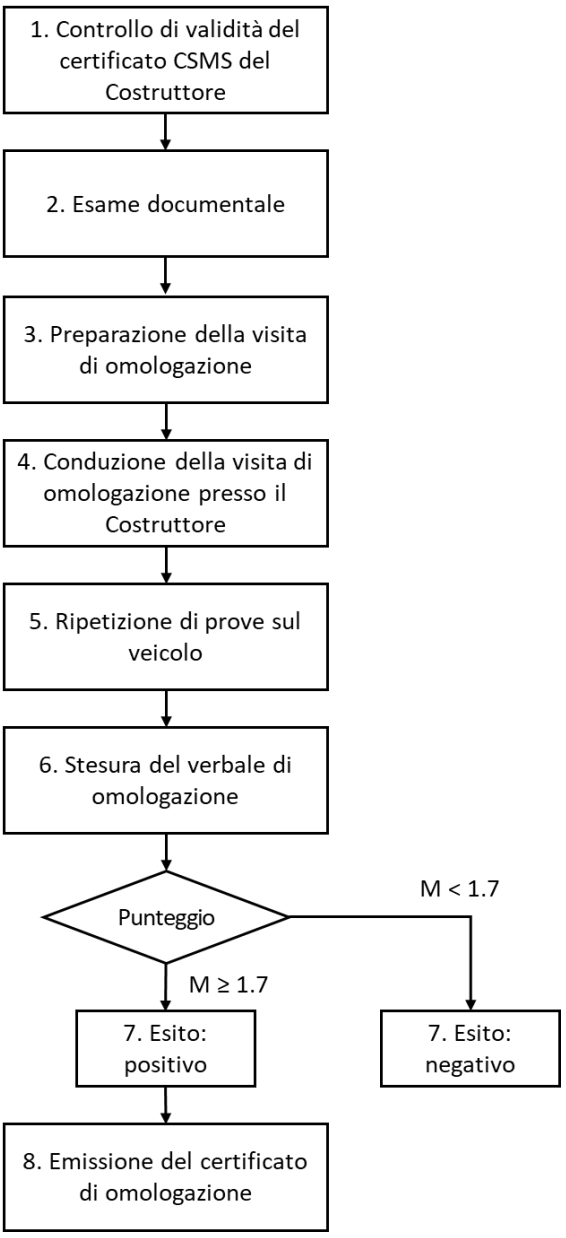


Figura 2 – Diagramma di flusso del processo di approvazione di tipo

Il Costruttore è tenuto a segnalare, tempestivamente, al Servizio Tecnico ogni modifica apportata al tipo di veicolo che richieda un aggiornamento o un'estensione dell'omologazione. Il Servizio Tecnico deciderà se sia sufficiente un esame documentale o se siano necessarie ulteriori visite e prove presso il Costruttore. Nel primo caso si tratterà di aggiornamento per revisione dell'omologazione, nel secondo di una estensione.

3.2 SCANSIONE TEMPORALE DEL PROCESSO

3.2.1 CRONOPROGRAMMA PER IL RILASCIO DEL CERTIFICATO CSMS

La pianificazione dell'audit CSMS, con l'indicazione dei tempi e delle risorse impiegate per ogni singola fase, è descritta nel dettaglio nella tabella 3.

Fase dell'audit CSMS	Durata (max)	Ruoli coinvolti
1. Esame documentale*	6 giorni	Presidente della Commissione Esperto di sicurezza informatica Esperto di sistemi di gestione
2. Preparazione dell'audit*	5 giorni	Presidente della Commissione Esperto di sicurezza informatica
3. Conduzione dell'audit presso il Costruttore*	5 giorni	Presidente della Commissione Esperto di sicurezza informatica Esperto di sistemi di gestione
4. Stesura del verbale di audit*	2 giorni	Presidente della Commissione Esperto di sistemi di gestione
5. Comunicazione dell'esito della valutazione	1 giorno	Presidente della Commissione
6. Rilascio del certificato CSMS	2 giorni	Responsabile dell'Autorità di omologazione
• In caso di esito condizionato dell'audit, il processo sarà ripetuto una sola volta, per le parti evidenziate in sede di audit stesso.		

Tabella 3 – Pianificazione audit CSMS

3.2.2 CRONOPROGRAMMA PER L'APPROVAZIONE DEL TIPO DI VEICOLO

La pianificazione delle attività di omologazione, con l'indicazione dei tempi e delle risorse impiegate per ogni singola fase, è descritta nel dettaglio nella tabella 4.

Fase dell'omologazione	Durata (max)	Ruoli coinvolti
1. Controllo di validità del certificato CSMS del Costruttore	2 giorni	Responsabile del Servizio Tecnico Esperto di sicurezza informatica
2. Esame documentale	3 giorni	Responsabile del Servizio Tecnico Esperto di sicurezza informatica Esperto di omologazione
3. Preparazione della visita di omologazione	2 giorni	Responsabile del Servizio Tecnico Esperto di sicurezza informatica
4. Conduzione della visita di omologazione presso il Costruttore	3 giorni	Responsabile del Servizio Tecnico Esperto di sicurezza informatica Esperto di omologazione
5. Ripetizione di prove sul veicolo	2 giorni	Responsabile del Servizio Tecnico Esperto di sicurezza informatica Esperto di omologazione
6. Stesura del verbale di omologazione	2 giorni	Responsabile del Servizio Tecnico Esperto di omologazione
7. Comunicazione dell'esito della valutazione	1 giorno	Responsabile del Servizio Tecnico
8. Emissione del certificato di omologazione	2 giorni	Responsabile dell'Autorità di omologazione

Tabella 4 – Pianificazione omologazione

3.3 CRITERI DI GIUDIZIO DELLA CONFORMITÀ

3.3.1 CRITERI PER IL RILASCIO DEL CERTIFICATO CSMS

Il giudizio sull'esito della valutazione sul CSMS del Costruttore, applicabile ai requisiti contenuti nel questionario di valutazione descritto nel par. 6.3, è basato su una valutazione a punteggio su tre livelli (2/1/0). L'esito della valutazione è basato sul calcolo della media, M, dei punteggi ottenuti.

Se $M < 1,4$ o in presenza di uno zero, l'esito della valutazione è negativo (non idoneo).

Se $1,4 \leq M < 1,7$ e in assenza di zeri, l'esito della valutazione è positivo con riserva. In questo caso il Servizio Tecnico richiede al Costruttore di attuare le necessarie azioni correttive e prevede un audit aggiuntivo, come indicato nel Diagramma di flusso in Figura 1 (ripetere).

Se $M \geq 1,7$ e in assenza di zeri, l'esito della valutazione è positivo (idoneo).

3.3.2 CRITERI PER L'APPROVAZIONE DEL TIPO DI VEICOLO

Il giudizio sull'esito della valutazione sul tipo di veicolo in approvazione, applicabile ai requisiti contenuti nel questionario di valutazione descritto nel par. 7.1, è basato su una valutazione a punteggio su tre livelli (2/1/0). L'esito della valutazione è basato sul calcolo della media, M, dei punteggi ottenuti.

Se $M < 1,7$ o in presenza di uno zero, l'esito della valutazione è negativo (non idoneo).

Se $M \geq 1,7$, e in assenza di zeri, l'esito della valutazione è positivo (idoneo).

All'esito positivo della valutazione deve, inoltre, corrispondere il superamento delle prove fisiche sul veicolo per le quali il Servizio Tecnico ha previsto la ripetizione in sede di visita di omologazione di cui al par. 7.2.

4. COMPETENZE DEL PERSONALE

4.1 COMPOSIZIONE DEI TEAM DI VALUTAZIONE

4.1.1 COMMISSIONE PER LA VALUTAZIONE DEL CSMS

La Commissione dell'audit CSMS è individuata dall'Autorità di omologazione ed è composta da:

- Presidente della Commissione e responsabile del procedimento;
- Esperto di sicurezza informatica;
- Esperto di sistemi di gestione.

La composizione della Commissione, con la descrizione dei compiti affidati ai singoli membri, è descritta nel dettaglio nella tabella 5.

Se un componente della Commissione è in possesso dei requisiti di cui al par. 4.2, tabella 7, la stessa persona può assumere più ruoli e il numero di componenti del personale incaricato si può ridurre a 2.

Ruolo	Numero	Responsabilità
Presidente della Commissione	1	È responsabile della programmazione e conduzione dell'audit. Prende le decisioni sull'esito dell'audit.
Esperto di sicurezza informatica	1	Supporta la Commissione con conoscenze specifiche nel settore della sicurezza informatica.
Esperto di sistemi di gestione	1	Supporta la Commissione con conoscenze ad ampio spettro dei sistemi di gestione aziendali e relativi processi.

Tabella 5 – Composizione Commissione

4.1.2 PERSONALE DEL SERVIZIO TECNICO PER L'APPROVAZIONE DELTIPO DI VEICOLO

I Servizi Tecnici abilitati all'esecuzione della visita di omologazione sono inquadrati nella categoria B ai sensi ai sensi dell'Accordo di Ginevra del 1958, scheda 2, Parte 1, punto 1.3., lettera b), e devono dimostrare di aver individuato, all'interno del proprio personale tecnico, risorse adeguatamente formate e in possesso dei necessari requisiti di competenza ed esperienza professionale.

Il personale incaricato per la visita di omologazione è individuato dal Servizio Tecnico ed è composto da:

- Responsabile del Servizio Tecnico e responsabile del procedimento;
- Esperto di sicurezza informatica;
- Esperto di omologazione.

La composizione del Servizio Tecnico, con la descrizione dei compiti affidati ai singoli membri, è descritta nel dettaglio nella tabella 6.

Se un componente del personale incaricato è in possesso dei requisiti di cui al par. 4.2, tabella 7, la stessa persona può assumere più ruoli e il numero di componenti del personale incaricato si può ridurre a 2.

Ruolo	Numero	Responsabilità
Responsabile del Servizio Tecnico	1	È responsabile della programmazione e conduzione della valutazione. Prende le decisioni sulle prove da ripetere e sull'esito della valutazione.
Esperto di sicurezza informatica	1	Supporta il responsabile del procedimento con conoscenze specifiche nel settore della sicurezza informatica.
Esperto di omologazione	1	Supporta il responsabile del procedimento con conoscenze amministrative e tecniche in merito ai processi di omologazione.

Tabella 6 – Composizione del Servizio Tecnico

4.1.3 SCAMBIO DI ESPERIENZE

Al fine di mantenere e, se possibile, incrementare le conoscenze nel settore da parte del personale coinvolto nei diversi processi, l'Autorità di omologazione favorirà lo scambio di esperienze, tramite piattaforma di comunicazione (es. Teams) fra il personale convolto al fine di perfezionare le procedure previste e promuoverà, nel caso, corsi specifici di aggiornamento.

4.2 REQUISITI PROFESSIONALI

La tabella 7 fornisce un'indicazione dei requisiti minimi di qualificazione, in ordine ai titoli di studio, alla formazione e all'esperienza professionale, in possesso dei componenti della Commissione e del Servizio Tecnico.

Ruolo	Titoli di studio	Esperienza professionale	Formazione specifica
Responsabile del procedimento	Laurea magistrale in ingegneria o architettura (o titoli equivalenti) e abilitazione all'esercizio della professione	5 anni di attività presso un Servizio Tecnico Ottime capacità relazionali, decisionali e di leadership	Corso specialistico di almeno 40 ore sul Reg. UN R155 e sulla ISO/SAE 21434
Esperto di sicurezza informatica	Laurea magistrale in ingegneria o architettura (o titoli equivalenti) e abilitazione all'esercizio della professione	5 anni di attività presso un Servizio Tecnico Approfondita conoscenza del Reg. UN R155 e delle norme sulla sicurezza informatica	Corso specialistico di almeno 40 ore sul Reg. UN R155 e sulla ISO/SAE 21434
Esperto di sistemi di gestione	Laurea magistrale in ingegneria o architettura (o titoli equivalenti) e abilitazione all'esercizio della professione	1 anno di attività presso un Servizio Tecnico Comprovata esperienza nella conduzione di audit Conformità del Prodotto	
Esperto di omologazione	Laurea magistrale in ingegneria o architettura (o titoli equivalenti) e abilitazione all'esercizio della professione	1 anno di attività presso un Servizio Tecnico Comprovata esperienza nella conduzione di visite ispettive e prove di omologazione	

Tabella 7 – Requisiti minimi di qualificazione

5. DOCUMENTI PER LA VALUTAZIONE

5.1 FASCICOLO DOCUMENTALE

In preparazione all'audit del CSMS e alla visita di omologazione, il Costruttore dovrà presentare al Servizio Tecnico un fascicolo documentale contenente il riferimento a tutti i documenti e le registrazioni utili a dimostrare di aver ottemperato a tutti i requisiti previsti dal Reg. UN R155.

Il fascicolo documentale sarà organizzato in modo da integrarsi perfettamente con i processi aziendali, pertanto, la sua struttura potrà variare anche sensibilmente da Costruttore a Costruttore.

Affinché il Servizio Tecnico possa accertarsi con maggiore facilità che tutti i documenti e le registrazioni utili alla dimostrazione della conformità ai requisiti siano effettivamente resi disponibili dal Costruttore, il fascicolo documentale dovrà essere corredato, in un allegato a margine, di una matrice di conformità redatta seguendo i criteri indicati nel par. 5.2.

5.1.1 FASCICOLO PER IL CSMS

Un elenco non esaustivo dei documenti e delle registrazioni che il Costruttore potrà richiamare nel fascicolo documentale e mettere a disposizione della Commissione, su richiesta, nel corso dell'audit CSMS è indicato nella Tabella 8.

Il costruttore, qualora fosse titolare di altro certificato di CSMS rilasciato da un'altra Autorità di omologazione, può presentarlo a corredo della documentazione.

Requisito	Descrizione	Criteri di valutazione	Evidenze richieste
6.2.	La domanda di certificato di conformità del sistema di gestione della cybersicurezza deve essere presentata dal costruttore del veicolo o da un mandatario accreditato del costruttore stesso.	Analisi e valutazione amministrativa delle istanze, in conformità all'allegato 2, ricevute via PEC.	Per le istanze via PEC è richiesta firma digitale valida per la pubblica amministrazione
6.3.1	Documenti che descrivono il sistema di gestione della cybersicurezza.	Analisi e valutazione tecnica della documentazione allegata dal costruttore in conformità all'allegato 2.	Approvazione dei dati forniti dal costruttore ritenuti esaustivi ai fini della caratterizzazione del sistema di gestione della cybersicurezza
7.2.2.1 7.2.2.2 7.2.2.3 7.2.2.4 7.2.2.5	Documentazione fornita dal costruttore necessaria alla valutazione dei processi e dei metodi utilizzati all'interno del CSMS.	Analisi e valutazione tecnica della documentazione allegata dal costruttore in conformità alla tabella 11 del paragrafo 6.3 (interpretazione dei requisiti per l'audit CSMS)	Valutazione documentale dei processi del Costruttore e, se del caso, controllo delle modalità utilizzate dal Costruttore per registrare le evidenze

Tabella 8 – Elenco non esaustivo dei documenti utili per l'audit CSMS

5.1.2 FASCICOLO PER L'APPROVAZIONE DEL TIPO DI VEICOLO

Un elenco non esaustivo dei documenti e delle registrazioni che il Costruttore potrà richiamare nel fascicolo documentale e mettere a disposizione del Servizio Tecnico, su richiesta, nel corso della visita di omologazione è indicato nella Tabella 9.

Requisito	Descrizione	Criteri di valutazione	Evidenze richieste
3.1	La domanda di omologazione di un tipo di veicolo per quanto riguarda la cybersicurezza deve essere presentata dal costruttore del veicolo o da un suo mandatario debitamente accreditato.	Analisi e valutazione amministrativa delle istanze, in conformità all'allegato 3, ricevute via PEC.	Le istanze devono essere firmate digitalmente e trasmesse via PEC
3.2.1	Descrizione del tipo di veicolo per quanto riguarda gli elementi specificati nell'allegato 1 del presente regolamento.	Analisi e valutazione tecnica della documentazione allegata dal costruttore in conformità all'allegato 3.	Approvazione dei dati forniti dal costruttore ritenuti esaustivi

			ai fini della caratterizzazione del tipo di veicolo
3.2.2	Nei casi in cui le informazioni sono coperte da diritti di proprietà intellettuale o costituiscono un know-how specifico del costruttore o dei suoi fornitori, il costruttore o i suoi fornitori devono mettere a disposizione informazioni sufficienti per effettuare correttamente i controlli di cui al presente regolamento. Tali informazioni devono essere trattate in via riservata.	Analisi e valutazione delle argomentazioni fornite dal Costruttore circa la riservatezza dei dati coperti da segreto industriale necessari ai sensi del presente Regolamento e che non possono essere divulgati liberamente senza il preventivo accordo con il Costruttore	Valutazione documentale delle dichiarazioni del Costruttore
7.3.2. 7.3.3. 7.3.4. 7.3.5. 7.3.6. 7.3.7. 7.3.8.	Documentazione fornita dal costruttore necessaria alla valutazione di processi e dei metodi utilizzati per gestire la cybersicurezza del tipo di veicolo da omologare.	Analisi e valutazione tecnica della documentazione allegata dal costruttore in conformità alla tabella 12 del paragrafo 7.1 (interpretazione dei requisiti per la valutazione di tipo)	Valutazione documentale dei processi del Costruttore e, se del caso, controllo delle modalità utilizzate dal Costruttore per registrare le evidenze
7.4.1.	Il costruttore del veicolo deve riferire almeno una volta all'anno, o più frequentemente se del caso, all'autorità di omologazione o al servizio tecnico in merito ai risultati delle sue attività di monitoraggio, quali definite al punto 7.2.2.2, lettera g), comprese le informazioni pertinenti sui nuovi attacchi informatici. Il costruttore del veicolo deve inoltre comunicare e confermare all'autorità di omologazione o al servizio tecnico che le misure di attenuazione in materia di cybersicurezza attuate in relazione ai suoi tipi di veicolo sono ancora efficaci e le eventuali azioni supplementari intraprese.	Analisi e valutazione dei report sulle attività di monitoraggio trasmessi dal costruttore tramite PEC	Valutazione documentale delle dichiarazioni del Costruttore Controllo delle modalità utilizzate dal Costruttore per registrare le evidenze

Tabella 9 – Elenco non esaustivo dei documenti utili per la visita di omologazione

5.2 MATRICE DI CONFORMITÀ

La matrice di conformità serve al singolo Costruttore per dimostrare al Servizio Tecnico che tutti i requisiti del Reg. UN R155 applicabili al CSMS e al tipo di veicolo in approvazione siano stati soddisfatti attraverso la loro opportuna integrazione all'interno dei processi aziendali.

L'Allegato 1 al presente documento contiene un esempio rappresentativo di una possibile struttura della matrice di conformità.

6. CRITERI SPECIFICI PER L'AUDIT CSMS

6.1 AUDIT PRESSO IL COSTRUTTORE

L'audit del CSMS viene condotto presso il Costruttore. In tal modo si può avere accesso a documenti di natura riservata che non possono essere condivisi altrimenti con l'Autorità di omologazione e si può valutare dal vivo l'effettiva attuazione dei processi aziendali da parte dell'organizzazione.

Nel caso più siti/stabilimenti siano interessati dai processi del CSMS, la Commissione concorderà con il Costruttore la sede o le sedi più adeguata/e presso la quale condurre l'audit.

6.2 NORME DI RIFERIMENTO

Non è richiesto che il Costruttore fornisca alcuna certificazione propedeutica alla conduzione dell'audit del CSMS. Tuttavia, il Costruttore deve fornire alla Commissione tutte le informazioni pertinenti ad eventuali certificati in corso di validità che attestino la conformità dell'organizzazione alle norme sui sistemi di gestione.

Un elenco non esaustivo delle norme di riferimento sui sistemi di gestione che possono essere utili in fase di audit CSMS è indicato nella tabella 10.

Riferimento/Numero	Titolo
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
ISO/SAE 21434:2021	Road vehicles — Cybersecurity engineering
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
ISO 26262 series	Road vehicles — Functional safety
ISO 9001:2015	Quality management systems — Requirements

Tabella 10 – Elenco non esaustivo delle norme utili per l'audit CSMS

6.3 INTERPRETAZIONE DEI REQUISITI PER L'AUDIT CSMS

La tabella 11 descrive il processo di verifica dei requisiti del Reg. UN R155 rilevanti per il CSMS.

Ad ogni singolo requisito in fase di audit sarà assegnato un punteggio (2/1/0), come descritto al par. 3.3.1.

UN R155	**Requisito**	**Interpretazione secondo ECE/TRANS/WP.29/2022/61**	**Esempi di documenti/prove che possono essere forniti (secondo ECE/TRANS/WP.29/2022/61)**
7.1.1.	Il costruttore del veicolo dispone di processi che verificano che le prescrizioni del presente regolamento non limitano le disposizioni o le prescrizioni di altri regolamenti ONU	I requisiti del presente regolamento non limitano le disposizioni o i requisiti di altri regolamenti ONU e le legislazioni nazionali o regionali come descritto ai punti 1.3 e 1.4 del campo di applicazione del presente Regolamento.	
7.2.1	Il Costruttore ha predisposto un'organizzazione aziendale, responsabilità e ambiti di competenza del personale addetto, risorse e misure opportune, piani di controllo	L'intento di questo requisito è che il servizio tecnico o l'autorità di omologazione verifichi che: (a) Il costruttore del veicolo disponga di un CSMS;	Possono essere applicabili i seguenti standard: (e) La norma ISO/SAE 21434 può essere utilizzata come base per evidenziare e valutare il CSMS. Le

	documentati, istruzioni per l'esecuzione dei test, gestione dei report, verifica dei risultati e controllo del piano per verificare che il sistema di gestione della cybersicurezza (CSMS) sia conforme al regolamento	(b) il CSMS presentato sia conforme ai requisiti elencati di seguito nel presente regolamento. Per questo requisito l'attenzione si concentra sui processi del costruttore e sulla valutazione della loro esistenza, al fine di ottenere una panoramica della capacità del costruttore di soddisfare i requisiti del CSMS. Si prega di notare i seguenti chiarimenti: (c) Il CSMS può essere parte del Sistema di gestione della qualità dell'organizzazione o essere indipendente da esso; (d) Se il CSMS è parte del SGQ dell'organizzazione, deve essere chiaramente identificabile.	clausole 5 "Gestione della cybersecurity organizzativa", 6 "Gestione della cybersecurity dipendente dal progetto" e 8 "Attività continue di cybersecurity" possono essere utilizzate per valutare il CSMS in generale; (f) le norme ISO 18045, ISO 15408, ISO 27000 e ISO 31000 possono essere applicabili a parti rilevanti del CSMS.
7.2.2.1.	Il costruttore del veicolo dispone di un sistema di gestione della cybersicurezza che si applica alle seguenti fasi: (a) fase di sviluppo, (b) fase di produzione, (c) fase di post-produzione	L'obiettivo di questo requisito è che il sistema di gestione della sicurezza informatica dovrebbe essere in grado di dimostrare come un costruttore gestirà la sicurezza informatica durante la vita operativa dei veicoli prodotti con un tipo di veicolo. Ciò include la dimostrazione che esistono procedure e processi implementati per coprire le tre fasi. Le diverse fasi del ciclo di vita possono avere attività specifiche da svolgere in ciascuna di esse. Il punto 7.2.2.1. descrive le diverse fasi del tipo di veicolo da considerare nel CSMS e il punto 7.2.2.2. si applica a tutte queste fasi se non diversamente indicato. Le fasi si applicano anche al punto 7.2.2.4. Il CSMS può includere processi o procedure attivi e/o reattivi che coprono la fine del supporto per un tipo di veicolo e come questo viene implementato o attivato. Può includere la possibilità di disconnettere funzioni/sistemi non obbligatori e in quali condizioni ciò potrebbe accadere. La vita operativa (fase di utilizzo) di un singolo veicolo inizierà durante la fase di produzione del tipo di veicolo. Terminerà durante la fase di produzione o la fase di post-produzione del tipo di veicolo.	Possono essere applicabili i seguenti standard: (a) ISO/SAE 21434 può essere utilizzato come base per evidenziare e valutare le fasi richieste del CSMS. Le clausole 9 "Concept", 10 "Product development" e 11 "Cybersecurity validation" possono essere utilizzate per valutare la fase di sviluppo del CSMS. La clausola 12 "Produzione" potrebbe essere utilizzata per valutare la fase di produzione del CSMS. Le clausole 8 "Attività continue di cybersecurity", 13 "Operazioni e manutenzione" e 14 "Fine del supporto alla cybersecurity e disattivazione" potrebbero essere utilizzate per valutare la fase di post-produzione del CSMS; (b) Altri standard che possono essere applicabili al 7.2.2. e ai suoi sotto-requisiti sono: ISO 18045, ISO 15408, serie ISO 27000, serie ISO 31000.
7.2.2.2.(a)	Il costruttore dispone di processi all'interno della propria organizzazione per gestire la cybersicurezza	Lo scopo di questo requisito è garantire che l'organizzazione disponga di processi per gestire l'attuazione del CSMS. Il suo ambito è limitato ai processi rilevanti per la sicurezza informatica dei tipi di veicoli e non ad altri aspetti dell'organizzazione. Ad esempio, l'ambito di applicazione di questo requisito non è inteso a coprire l'intera sicurezza delle informazioni del Sistema di gestione di un'organizzazione. Il requisito è da considerarsi non soddisfatto se una delle seguenti affermazioni è vera: 1. I processi sono assenti o incompleti. 2. I processi non vengono applicati universalmente o in modo coerente. 3. I processi vengono spesso o regolarmente aggirati per raggiungere gli obiettivi aziendali. 4. L'approccio alla governance della sicurezza e alla gestione del rischio del costruttore del veicolo non ha alcuna incidenza sui suoi processi. 5. La sicurezza del sistema dipende totalmente dall'applicazione attenta e	Quanto segue potrebbe essere utilizzato per mostrare la gamma di attività svolte dal costruttore per gestire la sicurezza informatica delle fasi di sviluppo, produzione e post-produzione di un tipo di veicolo: (a) Struttura organizzativa utilizzata per affrontare la sicurezza informatica; (b) Ruoli e responsabilità in materia di gestione della sicurezza informatica incl. responsabilità. Possono essere applicabili i seguenti standard: (c) La norma ISO/SAE 21434 può essere utilizzata come base per dimostrare e valutare quanto richiesto, in particolare sulla base di [RQ-05-01], [RQ-05-02], [RQ-05-06], [RQ-05-07]; (d) la BSI PAS 1885 potrebbe essere utilizzata per dimostrare questo requisito. Gli schemi di certificazione nazionali, come il Cyber Essentials del Regno Unito, potrebbero essere utilizzati per dimostrare i processi organizzativi di un produttore.

		coerente da parte degli utenti dei processi di sicurezza manuali. 6. I processi non sono stati rivisti in risposta a cambiamenti importanti (ad es. tecnologia o quadro normativo) o entro un periodo adeguato. 7. I processi non sono prontamente disponibili per il personale, troppo dettagliati da ricordare o troppo difficili da capire. Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere: 1. Il produttore del veicolo documenta in modo completo la sua governance della sicurezza generale e l'approccio di gestione del rischio, le pratiche di sicurezza tecnica e la conformità normativa specifica. La sicurezza informatica è integrata e incorporata in tutti questi processi e gli indicatori chiave di prestazione sono segnalati alla sua direzione esecutiva. 2. I processi del costruttore del veicolo sono sviluppati per essere pratici, utilizzabili e adeguati alle sue politiche e tecnologie. 3. I processi che si basano sul comportamento dell'utente sono pratici, appropriati e realizzabili. 4. Il produttore del veicolo rivede e aggiorna i processi a intervalli adeguatamente regolari per garantire che rimangano pertinenti. Questo si aggiunge alle recensioni a seguito di un grave incidente di sicurezza informatica. 5. Qualsiasi modifica alla funzione essenziale o alla minaccia che deve affrontare innesca una revisione processi. 6. I sistemi del produttore del veicolo sono progettati in modo che siano e rimangano sicuri anche quando le politiche e i processi di sicurezza degli utenti non vengono sempre seguiti. Per tale affermazione dovrebbe essere fornita una giustificazione.	
7.2.2.2.(b)	Il costruttore dispone di processi utilizzati per l'identificazione dei rischi per i tipi di veicolo Nell'ambito di tali processi prende in considerazione le minacce di cui all'Allegato 5, Parte A del Regolamento e altre minacce pertinenti	Lo scopo di questo requisito è che un costruttore dimostri i processi e le procedure che utilizza per identificare i rischi per i tipi di veicoli. I processi implementati dovrebbero considerare tutte le probabili fonti di rischio. Ciò include i rischi identificati nell'allegato 5 del regolamento sulla sicurezza informatica, ad esempio i rischi derivanti da servizi connessi o dipendenze esterne al veicolo. I processi possono considerare: (d) Identificazione della rilevanza di un sistema per la sicurezza informatica; (e) Descrizione del sistema complessivo rispetto a: (i) Definizione del sistema/funzione; (ii) Confini e interazioni con altri sistemi; (iii) Architettura; (iv) Ambiente di funzionamento del sistema (contesto, vincoli e ipotesi). (f) Identificazione dei beni; (g) Identificazione delle minacce; (h) Identificazione delle vulnerabilità. Il requisito è da considerarsi non soddisfatto se una delle seguenti affermazioni è vera: 1. L'identificazione del rischio non si basa su un insieme chiaramente definito di ipotesi.	Possono essere indicate le fonti per l'identificazione del rischio. Questi possono includere: (a) Piattaforme di condivisione di vulnerabilità/minacce; (b) Lezioni apprese riguardo a rischi e vulnerabilità. Possono essere applicabili i seguenti standard: (c) ISO/SAE 21434, in particolare sulla base di [RQ-15-01], [RQ-15-02], [RQ-15-03], [RQ-15-08].

		2. L'identificazione del rischio per i tipi di veicoli è un'attività "una tantum" (o non viene eseguita affatto). 3. I tipi di veicoli vengono valutati in isolamento, senza considerare le dipendenze e le interazioni con altri sistemi. (es. interazioni tra ambienti IT e OT). Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere: 1. Il processo organizzativo del produttore del veicolo garantisce che i rischi per la sicurezza dei tipi di veicolo siano identificati, analizzati, prioritizzati e gestiti. 2. L'approccio del produttore del veicolo al rischio è incentrato sulla possibilità di un impatto negativo sui suoi tipi di veicolo, portando a una comprensione dettagliata di come tale impatto potrebbe verificarsi in conseguenza di possibili azioni di un aggressore e delle proprietà di sicurezza delle sue reti e dei suoi sistemi. 3. L'identificazione del rischio da parte del costruttore del veicolo si basa su una serie di presupposti chiaramente compresi, basati su una comprensione aggiornata delle minacce alla sicurezza dei suoi tipi di veicoli e del suo settore. 4. L'identificazione del rischio da parte del costruttore del veicolo è basata sulla comprensione delle vulnerabilità dei suoi tipi di veicolo. 5. Il produttore del veicolo esegue un'analisi dettagliata delle minacce e comprende come ciò si applica alla tua organizzazione nel contesto della minaccia ai suoi tipi di veicoli e al suo settore.	
7.2.2.2.(c)	Il costruttore dispone di processi utilizzati per la valutazione, la categorizzazione e il trattamento dei rischi individuati	Lo scopo di questo requisito è che il fabbricante dimostri i processi e le regole che utilizza per valutare, classificare e trattare i rischi identificati. I processi possono considerare: (c) Valutare l'impatto associato relativo ai rischi identificati nel requisito 7.2.2.2.b); (d) Identificazione di potenziali percorsi di attacco relativi ai rischi identificati nel requisito 7.2.2.2. b); (e) Determinazione della fattibilità/probabilità di attacco per ogni percorso di attacco sopra individuato; (f) Calcolo e categorizzazione dei rischi; (g) Opzioni di trattamento dei rischi identificati e classificati. Il requisito è da considerarsi non soddisfatto se una delle seguenti affermazioni è vera: 1. I risultati della valutazione del rischio sono troppo complessi o ingombranti per essere utilizzati dai responsabili delle decisioni e non vengono comunicati in modo efficace in modo chiaro e tempestivo. 2. I requisiti di sicurezza e le tecniche di mitigazione sono arbitrari o vengono applicati da un catalogo di controllo senza considerare come contribuiscono alla sicurezza dei tipi di veicoli. 3. Solo alcuni domini o tipi di asset sono documentati e compresi. Le dipendenze tra le risorse non vengono comprese (come le dipendenze tra IT e OT). 4. Le rimanenze di attività relative ai tipi di veicoli sono incomplete, inesistenti o non adeguatamente dettagliate. 5. Le scorte di beni sono trascurate e non aggiornate.	Possono essere applicabili i seguenti standard: (a) ISO/SAE 21434, in particolare sulla base di [RQ-15-15], [RQ-15-16], [RQ-15-04]. [RQ-15-05], [RQ-15-10], [RQ-15-17], [RQ-09-05], [RQ-09-06]; (b) la BSI PAS 11281:2018 può essere applicabile per la considerazione della sicurezza e della protezione.

		6. I sistemi vengono valutati in isolamento, senza considerare le dipendenze e le interazioni con altri sistemi (ad es. interazioni tra ambienti IT e OT). 7. Le valutazioni del rischio non si basano su un insieme chiaramente definito di ipotesi. 8. Le valutazioni del rischio per i tipi di veicoli sono un'attività "una tantum" (o non vengono eseguite affatto). Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere: 1. L'output del processo di gestione dei rischi del costruttore del veicolo è un chiaro insieme di requisiti di sicurezza che affronteranno i rischi in linea con la sua organizzazione approccio alla sicurezza. 2. Tutti i beni rilevanti per il funzionamento sicuro dei suoi tipi di veicoli sono identificati e inventariati (a un livello di dettaglio adeguato). 3. L'inventario è tenuto aggiornato. 4. Le dipendenze dall'infrastruttura di supporto sono riconosciute e registrate. 5. Il costruttore del veicolo ha assegnato la priorità agli asset in base alla loro importanza per il funzionamento dei suoi tipi di veicolo. 6. L'identificazione del rischio da parte del costruttore del veicolo si basa su una serie di presupposti chiaramente compresi, basati su una comprensione aggiornata delle minacce alla sicurezza dei suoi tipi di veicoli e del suo settore. 7. L'identificazione del rischio da parte del costruttore del veicolo è basata sulla comprensione delle vulnerabilità nei suoi tipi di veicoli. 8. Il produttore può dimostrare l'efficacia e la ripetibilità dei propri processi per la categorizzazione e il trattamento del rischio.	
7.2.2.2.(d)	Il costruttore dispone di processi per verificare che i rischi individuati siano gestiti in modo adeguato	Lo scopo di questo requisito è che il fabbricante dimostri i processi e le regole che utilizza per decidere come gestire i rischi. Ciò può includere i criteri decisionali per il trattamento del rischio, ad esempio il processo per selezionare quali controlli implementare e quando accettare un rischio. I risultati del processo di identificazione e valutazione dei rischi dovrebbero contribuire alla selezione delle opzioni di categoria di trattamento appropriate per affrontare tali rischi. Il risultato di questo processo dovrebbe essere che il rischio residuo (rischi rimanenti dopo il trattamento) rientri nella tolleranza ai rischi dichiarata dal produttore (cioè entro i limiti accettabili dichiarati). Nei processi devono essere considerate le mitigazioni individuate nell'allegato 5 del regolamento sulla sicurezza informatica. I processi possono considerare: (c) metodologie di trattamento del rischio appropriate e proporzionate; (d) il trattamento degli elementi critici (con sicurezza e ambiente) per garantire che i rischi per essi siano adeguatamente mitigati e proporzionalmente basato sull'obiettivo di sicurezza o ambientale dei sistemi di veicoli dipendenti; (e) garantire che il rischio residuo rimanga entro limiti accettabili per i componenti o per il tipo generale di veicolo;	Possono essere applicabili i seguenti standard: (a) ISO/SAE 21434 può essere utilizzata come base per l'evidenza e la valutazione come richiesto, in particolare sulla base di [RQ-09-07], [RQ-09-11] e [RQ-11-01]; (b) la ISO 31000 può essere applicabile se adattata ai rischi legati al prodotto.

		(f) Dettagliare tutti i casi in cui l'organizzazione accetterebbe la giustificazione per il mancato rispetto della loro dichiarata tolleranza al rischio. Il requisito è da considerarsi non soddisfatto se una delle seguenti affermazioni è vera: 1. Gli elementi di sicurezza dei progetti o dei programmi dipendono esclusivamente dal completamento di una valutazione della gestione del rischio, indipendentemente dai risultati. 2. Non esiste un processo sistemico in atto per garantire che i rischi per la sicurezza identificati siano gestiti in modo efficace. 3. I rischi rimangono irrisolti su un registro per periodi di tempo prolungati in attesa che il processo decisionale senior o l'allocazione delle risorse si risolvano. Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere: 1. Le conclusioni significative raggiunte nel corso del processo di gestione del rischio del costruttore del veicolo vengono comunicate ai principali responsabili delle decisioni in materia di sicurezza e alle persone responsabili. 2. L'efficacia del processo di gestione del rischio del costruttore del veicolo viene riesaminata periodicamente e, se necessario, i miglioramenti apportati.	
7.2.2.2.(e)	Il costruttore dispone di processi utilizzati per testare la cybersicurezza di un tipo di veicolo	L'obiettivo di questo requisito è garantire che il produttore disponga di capacità e processi adeguati a testare il tipo di veicolo durante le sue fasi di sviluppo e produzione. I processi di test in fase di produzione possono essere diversi da quelli utilizzati in fase di sviluppo. I processi possono considerare: Fase di sviluppo: (c) Regole specifiche dell'organizzazione per i test durante lo sviluppo; (d) Processi per la creazione e l'esecuzione di strategie di test; (e) Processi per la pianificazione dei test di sicurezza informatica; (f) Processi per test di progettazione di sistemi di sicurezza informatica; (g) Processi per test di unità software di sicurezza informatica; (h) Processi per test hardware di sicurezza informatica; (i) Processi per test di integrazione della sicurezza informatica; (j) Processi per la documentazione dei risultati delle prove; (k) Processi per la gestione delle vulnerabilità individuate durante i test; (l) Giustificazione e requisiti per i test di sicurezza informatica, come test funzionali (basati sui requisiti, positivi e negativi), test di interfaccia, test di penetrazione, scansione delle vulnerabilità, test fuzz ma non limitati agli stessi. Fase di produzione: (m) Processi di test volti a garantire che il sistema prodotto disponga della sicurezza informatica requisiti, controlli e capacità delineati nel piano di produzione; (n) Processi di test per garantire che l'articolo prodotto soddisfi le specifiche di	Possono essere applicabili i seguenti standard: (a) ISO/SAE 21434 può essere utilizzato come base per evidenziare e valutare come richiesto, in particolare sulla base di, [RQ-10-09], [RQ-10-10], [RQ-11-01]; (b) la BSI PAS 11281:2018 può essere utilizzata per considerare l'interazione tra sicurezza e protezione e i processi per dimostrare che i risultati della sicurezza sono soddisfatti.

		cybersecurity che sono conformi al sistema in fase di sviluppo; (o) Processi di test per garantire che i controlli di sicurezza informatica e la configurazione come specifiche di sicurezza informatica siano abilitati nell'articolo prodotto; (p) Processi per la documentazione dei risultati del test e la gestione dei risultati. Il requisito è da considerarsi non soddisfatto se una delle seguenti affermazioni è vera: 1. Un particolare prodotto o servizio è visto come un "proiettile d'argento" e le affermazioni del venditore sono prese per valore nominale. 2. I metodi di garanzia vengono applicati senza apprezzarne i punti di forza e i limiti, come i rischi dei test di penetrazione negli ambienti operativi. 3. Si presume l'assicurazione perché non ci sono stati problemi noti fino ad oggi. Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere: 1. Il costruttore del veicolo convalida che le misure di sicurezza in atto per proteggere i sistemi siano efficaci e rimangano efficaci fino alla fine del ciclo di vita di tutti i veicoli con i tipi di veicolo per i quali sono necessari. 2. Il costruttore del veicolo comprende i metodi di garanzia a sua disposizione e sceglie i metodi appropriati per acquisire fiducia nella sicurezza dei tipi di veicolo. 3. La fiducia del costruttore del veicolo nella sicurezza in relazione alla sua tecnologia, persone e processi può essere giustificata e verificata da una terza parte. 4. Deficit di sicurezza scoperti da valutati, prioritizzati e risolti, se necessario, in modo tempestivo ed efficace. 5. I metodi utilizzati per l'assicurazione vengono riesaminati per garantire che funzionino come previsto e rimangano il metodo più appropriato da utilizzare.	
7.2.2.2.(f)	Il costruttore dispone di processi utilizzati per garantire che la valutazione del rischio sia mantenuta aggiornata	Lo scopo di questo requisito è garantire che la valutazione del rischio sia mantenuta aggiornata. Ciò dovrebbe includere processi per identificare se i rischi per un tipo di veicolo sono cambiati e come questo sarà considerato nella valutazione del rischio. Si segnala che i requisiti 7.2.2.2. le parti da f) ad h) possono presentare sovrapposizioni in termini di processi utilizzati e pertanto le stesse prove possono essere applicabili per dimostrare che tali requisiti sono soddisfatti. Il requisito è da considerarsi non soddisfatto se la seguente affermazione è vera: 1. Non sono in essere processi che richiedano l'aggiornamento della valutazione del rischio. Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere: 1. Il produttore del veicolo effettua le valutazioni del rischio quando eventi significativi potenzialmente influiscono sui tipi di veicolo, come la sostituzione di un sistema o un cambiamento nella minaccia alla sicurezza informatica. 2. Le valutazioni del rischio del costruttore del veicolo sono dinamiche e aggiornate alla luce delle modifiche pertinenti che possono	Possono essere indicate le fonti per l'identificazione del rischio. Questi possono includere: (a) Piattaforme di condivisione di vulnerabilità/minacce; (b) Lezioni apprese in merito a rischi e vulnerabilità (c) Conferenze. (d) la norma ISO/SAE 21434 può essere utilizzata come base per evidenziare e valutare come richiesto, in particolare sulla base di [RQ-08-07] [RQ-06-09], [RQ-07-06].

		includere modifiche tecniche ai tipi di veicoli, modifiche all'uso e nuove informazioni sulle minacce.	
7.2.2.2.(g)	Il costruttore dispone di processi utilizzati per monitorare, individuare e rispondere agli attacchi e minacce informatiche e alle vulnerabilità dei tipi di veicolo e di processi utilizzati per valutare se le misure di cybersicurezza attuate siano ancora efficaci alla luce delle nuove minacce informatiche e vulnerabilità individuate	L'obiettivo di questo requisito è garantire che il produttore disponga di processi per monitorare attacchi informatici, minacce o vulnerabilità ai veicoli che il produttore ha omologato, ovvero si trovano nella fase di post-produzione o produzione, e che abbia stabilito processi che permetterebbe loro di rispondere in modo appropriato e tempestivo. Si segnala che i requisiti 7.2.2.2. le parti da f) ad h) possono presentare sovrapposizioni in termini di processi utilizzati e pertanto le stesse prove possono essere applicabili per dimostrare che tali requisiti sono soddisfatti. Il requisito è da considerarsi non soddisfatto se una delle seguenti affermazioni è vera: 1. Il produttore del veicolo non dispone di fonti di intelligence sulle minacce. 2. Il produttore del veicolo non applica gli aggiornamenti in modo tempestivo, dopo averli ricevuti. 3. Il produttore del veicolo non valuta l'utilità della propria intelligence sulle minacce né condivide feedback con fornitori, fornitori di servizi aftermarket autorizzati o altri utenti. 4. Non vi è personale che svolga una funzione di monitoraggio. 5. Il personale addetto al monitoraggio non ha le competenze specialistiche corrette. 6. Il personale addetto al monitoraggio non è in grado di riferire in merito ai requisiti di governance. 7. Gli avvisi di sicurezza relativi ai tipi di veicoli non hanno la priorità. Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere: 1. Vengono raccolti dati relativi alla sicurezza e al funzionamento dei tipi di veicoli. 2. Gli avvisi di terze parti vengono esaminati e vengono intraprese azioni. 3. Alcuni set di dati di registrazione possono essere facilmente interrogati con strumenti di ricerca per facilitare le indagini. 4. La risoluzione degli avvisi a una risorsa o sistema viene eseguita regolarmente. 5. Gli avvisi di sicurezza relativi ai tipi di veicoli hanno la priorità. 6. Il produttore del veicolo applica gli aggiornamenti in modo tempestivo. 7. Il produttore di veicoli dispone di processi per monitorare, rilevare e rispondere ad attacchi informatici, minacce informatiche e vulnerabilità rilevanti per le sue esigenze aziendali o minacce specifiche nel suo settore. 8. Il produttore del veicolo sa quanto sono efficaci i suoi processi (ad esempio monitorando come lo aiutano a identificare i problemi di sicurezza). 9. Il personale addetto al monitoraggio ha adeguate capacità investigative e una conoscenza di base dei dati con cui deve lavorare. 10. Il personale addetto al monitoraggio può riferire ad altre parti dell'organizzazione (ad es. direttori della sicurezza, responsabili della resilienza).	Possono essere applicabili i seguenti standard: (a) ISO/SAE 21434 può essere utilizzata come base per evidenziare e valutare come richiesto, in particolare sulla base di [RQ-08-01], [RQ-08-02]. [RQ-08-03], [RQ-08-04], [RQ-08-05], [RQ-08-07], [RQ-08-08], [RQ-07-06], [RC-07-08], [RQ-13-01] e [RQ-13-02]. Quanto segue potrebbe essere utilizzato per evidenziare i processi utilizzati: (b) Processi di monitoraggio della sicurezza informatica per i veicoli in post-produzione. Ciò può includere processi che raccolgono informazioni che possono o non possono essere pertinenti al veicolo/sistema del produttore; (c) Processi di valutazione delle informazioni sulla sicurezza informatica. Si tratta di processi per l'identificazione della rilevanza delle informazioni raccolte rispetto al sistema/veicolo del costruttore; (d) Processi per la determinazione/valutazione del rischio per le informazioni rilevanti; (e) Procedure di risposta agli incidenti per entrambi i veicoli già immatricolati e non ancora immatricolati dei tipi di veicoli coperti dal CSMS, che possono includere prove di procedure per: (i)Interazione con le autorità; (ii) Attivatori identificati o dichiarati che porterebbero a un'escalation o ad un'azione; (iii) Determinare quali opzioni di risposta potrebbero essere implementate per quali condizione; (iv) Gestire eventuali dipendenze e interazioni con i fornitori. (f) Prova che le procedure di risposta funzionerebbero, ad esempio attraverso l'esercizio e la verifica che le ipotesi di pianificazione rimangano valide durante il test.

		11. Il costruttore del veicolo dimostra con successo i processi per valutare se le misure di sicurezza informatica implementate sono sufficientemente solide da concludere se sono ancora efficaci.	
7.2.2.2.(h)	Il costruttore dispone di processi utilizzati per fornire dati pertinenti a sostegno dell'analisi di attacchi informatici tentati o riusciti	L'obiettivo di questo requisito è garantire che sia stato stabilito un processo per fornire i dati necessari per l'analisi e le responsabilità associate per la gestione dei dati e dell'analisi.	(a) La norma ISO/SAE 21434 può essere utilizzata come base per l'evidenza e la valutazione come richiesto, in particolare sulla base di [RQ-08-03], [RQ-08-04]. I seguenti documenti potrebbero essere utilizzati per dimostrare i processi utilizzati: (b) Procedura per l'implementazione delle attività del Security Incident Response Team (incidenti); (c) Monitoraggio sul campo (ottenimento di informazioni su incidenti e vulnerabilità); (d) Procedura quando si verifica un incidente (compresa una panoramica di quali informazioni vengono trasmesse all'analista in quali fasi); (e) Procedura in caso di scoperta di una vulnerabilità (compresa una panoramica delle informazioni trasmesse all'analista in quali fasi).
7.2.2.3.	Il costruttore dispone di processi utilizzati nel suo sistema di gestione della cybersicurezza che, sulla base della categorizzazione riferite ai commi (c) e (g) del punto 7.2.2.2, garantiranno che le minacce informatiche e le vulnerabilità siano attenuate entro un lasso di tempo ragionevole	L'intento di questo requisito è quello di garantire che, dopo la classificazione dei rischi identificati, sia stato stabilito un processo per determinare il termine di risposta in base ai risultati della classificazione. È necessario stabilire il termine di risposta attraverso processi come il triage e spiegare il processo di monitoraggio per verificare se viene eseguito entro il termine. Le tempistiche fornite dai produttori devono poter essere giustificate e spiegate. Potrebbe esserci una serie di tempistiche che coprono diverse situazioni possibili. Questo dovrebbe includere i tempi per decidere e attuare le possibili reazioni o risposte.	La norma ISO/SAE 21434 può essere utilizzata come base per dimostrare i processi richiesti, in particolare sulla base di [RQ-08-07] e [RQ-08-08]. I seguenti documenti possono essere utilizzati per dimostrare i processi utilizzati: (a) Procedura per l'implementazione delle attività di risposta agli incidenti di sicurezza informatica, tra cui: (i) Monitoraggio sul campo (ottenimento di informazioni su incidenti e vulnerabilità); (ii) Procedura per la gestione degli incidenti, compresa la determinazione dei tempi di risposta; (iii) procedure per scoprire le vulnerabilità. (b) Dimostrazione di come vengono attuate le procedure.
7.2.2.4.	Il costruttore dispone di processi utilizzati all'interno del proprio sistema di gestione della cybersicurezza che garantiscono che il monitoraggio riferito al comma (g) del punto 7.2.2.2. sia continuo, includa i veicoli dopo la prima immatricolazione e sia capace di analizzare e rilevare minacce informatiche, vulnerabilità e attacchi attraverso i dati e i log dei veicoli	L'obiettivo di questo requisito è garantire che i processi di monitoraggio degli attacchi informatici, delle minacce informatiche e delle vulnerabilità sui tipi di veicoli siano continui e si applichino a tutti veicoli immatricolati del produttore che rientrano nell'ambito del loro sistema di gestione della sicurezza informatica e utilizzo: (a) le informazioni sul monitoraggio acquisite ai sensi del punto 7.3.7. oltre altre fonti di informazione sul monitoraggio acquisite in conformità al punto 7.2.2.2. (g) (come i social media). Si segnala che il paragrafo 1.3., e il rispetto delle leggi sulla privacy dei dati, sono particolarmente rilevanti per questo requisito.	La norma ISO/SAE 21434 può essere utilizzata come base per l'evidenza e la valutazione come richiesto, in particolare sulla base dei punti 8.3 "Monitoraggio della cybersecurity", 8.4 "Valutazione degli eventi di cybersecurity", 8.5 "Analisi delle vulnerabilità". I seguenti documenti possono essere utilizzati per dimostrare i processi utilizzati: (b) Procedura per l'attuazione delle attività di risposta agli incidenti di sicurezza informatica, tra cui: (i) monitoraggio sul campo (ottenimento di informazioni su incidenti e vulnerabilità) (ii) procedura per la gestione degli incidenti (iii) Procedure per scoprire le vulnerabilità. (c) Dimostrazione di come vengono attuate le procedure.
7.2.2.5.	Il costruttore ha dimostrato in che modo il suo sistema di gestione della	L'intento di questo requisito è garantire che si possa dimostrare che i rischi dei fornitori	Possono essere applicabili i seguenti standard:

	cybersicurezza gestirà le eventuali dipendenze con fornitori, fornitori di servizi o sub-organizzazioni del costruttore per quanto riguarda le prescrizioni riferite al punto 7.2.2.2.	possono essere conosciuti e possono essere gestiti nell'ambito dei processi descritti nel CSMS. Le misure adottate dovrebbero essere proporzionate ai rischi derivanti da ciò che viene fornito. L'attuazione finale dei processi può essere incorporata in un accordo bilaterale tra il costruttore del veicolo ei suoi fornitori. All'interno del CSMS possono essere presenti processi per: (a)identificare i rischi associati a parti, componenti, sistemi o servizi forniti dai fornitori; (b) gestire i rischi per il veicolo derivanti da fornitori di servizi che forniscono funzioni di connettività o servizi su cui un veicolo può fare affidamento, ciò può includere ad esempio fornitori di servizi cloud, fornitori di telecomunicazioni, fornitori di Internet e fornitori di servizi aftermarket autorizzati; (c) garantire che i fornitori a contratto e/o i fornitori di servizi siano in grado di dimostrare come hanno gestito i rischi ad essi associati. I processi possono includere la considerazione di requisiti di convalida o test che possono essere utilizzati per dimostrare che i rischi sono gestiti in modo appropriato; (d) delegare i requisiti pertinenti ai dipartimenti o alle sub-organizzazioni competenti del fabbricante, al fine di gestire i rischi identificati. Si noti che è possibile imporre requisiti ai fornitori di livello 1 e richiederli a cascata ai fornitori di livello 2. Tuttavia, può essere difficile per un produttore inserire i requisiti più in basso nella catena di approvvigionamento (in particolare i requisiti giuridicamente vincolanti). Il requisito è da considerarsi non soddisfatto se la seguente affermazione è vera 1. I contratti pertinenti con fornitori e fornitori di servizi non hanno requisiti di sicurezza informatica. Il requisito può considerarsi soddisfatto se tutte le seguenti affermazioni sono vere 1. Il produttore di veicoli ha una profonda conoscenza della sua catena di approvvigionamento, compresi i subappaltatori e i rischi più ampi che deve affrontare. Il produttore del veicolo considera fattori quali le partnership del fornitore, i concorrenti, la nazionalità e altre organizzazioni con cui subappalta. Ciò informa i suoi processi di valutazione del rischio e di approvvigionamento. 2. L'approccio del produttore di veicoli alla gestione del rischio della catena di approvvigionamento considera i rischi per i suoi tipi di veicoli derivanti dalla sovversione della catena di approvvigionamento da parte di aggressori capaci e dotati di risorse adeguate. 3. Il produttore del veicolo è sicuro che le informazioni condivise con i fornitori, essenziali per il funzionamento dei tipi di veicolo, siano adeguatamente protette da attacchi sofisticati. 4. Il costruttore del veicolo può esprimere chiaramente le esigenze di sicurezza che pone ai fornitori in modi che siano	(e) La norma ISO/SAE 21434 può essere utilizzata come base per evidenziare e valutare come richiesto, in particolare sulla base di [RQ-06-10], [RQ-07-04], [RC-07-05]. Per comprovare i processi utilizzati si possono utilizzare i seguenti elementi: (f) Accordi contrattuali in essere o prove di tali accordi; (g) argomentazioni comprovate su come i loro processi garantiranno che i fornitori/fornitori di servizi siano presi in considerazione nel processo di valutazione del rischio; (h) Procedure/Metodi di condivisione delle informazioni sui rischi tra fornitori e produttori; (i) Soluzioni/contratti esistenti come la normativa ISMS (Information Security Management System) possono essere utilizzati come prova. Questo può essere dimostrato da certificati basati su ISO/IEC 27001 o TISAX (Trusted Information Security Assessment eXchange).

		reciprocamente compresi e stabiliti nei contratti. Esiste un modello di responsabilità condivisa chiaro e documentato. 5. Tutte le connessioni di rete e la condivisione dei dati con terze parti sono gestite in modo efficace e proporzionato. 6. Se del caso, il processo di gestione degli incidenti del costruttore del veicolo e quello dei suoi fornitori forniscono supporto reciproco nella risoluzione degli incidenti.	

Tabella 11 – Lista di riscontro per l'audit CSMS

7. CRITERI SPECIFICI PER LA VALUTAZIONE DEL TIPO DI VEICOLO

7.1 INTERPRETAZIONE DEI REQUISITI PER LA VALUTAZIONE DEL TIPO DI VEICOLO

La tabella 12 descrive il processo di verifica dei requisiti del Reg. UN R155 rilevanti per la valutazione di tipo. Ad ogni singolo requisito in fase di audit sarà assegnato un punteggio (2/1/0), come descritto al par. 3.3.2.

UN R155	**Requisito**	**Interpretazione secondo ECE/TRANS/WP.29/2022/61**	**Esempi di documenti/prove che possono essere forniti (secondo ECE/TRANS/WP.29/2022/61)**
7.3.1.	Il costruttore è in possesso di un certificato di conformità valido* per il sistema di gestione della cybersicurezza relativo al tipo di veicolo da omologare *Per le omologazioni anteriori al 1° luglio 2024, il costruttore non è obbligato a produrre un certificato di conformità valido, ma dimostra che la cybersicurezza è stata presa in considerazione durante la fase di sviluppo del tipo di veicolo in questione	L'obiettivo di questo requisito è garantire che vi sia un certificato di conformità valido per CSMS per consentire il rilascio dell'omologazione per qualsiasi nuovo tipo di veicolo e che sia appropriato al tipo di veicolo. Per architetture esistenti che sono state sviluppate prima di ottenere il certificato CSMS potrebbe non esser stato possibile sviluppare l'architettura in piena conformità con il relativo CSMS. Pertanto, per omologazioni anteriori al 1° luglio 2024, le prescrizioni relative alla "considerazione adeguata" della sicurezza informatica si applicano limitatamente alla fase di sviluppo. Le fasi di produzione e post-produzione di quei tipi di veicolo devono essere pienamente conformi al CSMS certificato. Ulteriori modifiche o aggiornamenti di natura tecnica che richiedano estensioni al tipo esistente posteriormente al 1° luglio 2024 dovrebbero aderire il più possibile ai processi definiti nel CSMS per la fase di sviluppo. Laddove vi siano scostamenti dai processi definiti nel CSMS questi dovrebbero essere illustrati e giustificati al servizio tecnico o all'autorità di omologazione e il management del costruttore dovrà assumersene la responsabilità ad un livello appropriato. Si noti il seguente chiarimento: (a) "relativo al tipo di veicolo da omologare" significa che il CSMS deve essere applicabile al tipo di veicolo da omologare.	Per dimostrare la validità del certificato CSMS si possono utilizzare i seguenti documenti: (b) Il certificato di conformità del CSMS per dimostrare che è ancora valido; (c) La conferma che il CSMS è applicato in modo appropriato al tipo di veicolo e tutte le informazioni necessarie per fornire garanzie. (d) Informazioni su come vengono gestiti gli aggiornamenti o le estensioni all'interno del CSMS per qualsiasi aggiornamento delle omologazioni prima del 1° luglio 2024".
7.3.2.	Il costruttore del veicolo ha individuato e gestito, per il tipo di veicolo da omologare, i rischi connessi ai fornitori	Questo requisito si riferisce specificamente all'acquisizione di informazioni sufficienti dalla catena di approvvigionamento ed è collegato a 7.2.2.5. Lo scopo di questo requisito è garantire che le informazioni presentate	Possono essere applicabili i seguenti standard: (a) ISO/SAE 21434. Per comprovare i processi utilizzati possono essere utilizzati i seguenti elementi:

		(insieme a quelle del costruttore) siano sufficienti per consentire una valutazione dei requisiti 7.3.3. a 7.3.6. Si noti il seguente chiarimento: (a) "rischi connessi ai fornitori" - L'obiettivo è che si possa dimostrare che i rischi dei fornitori possono essere conosciuti e gestiti. Si ammette che è difficile far scendere i requisiti a cascata nella catena di fornitura oltre i fornitori di livello 2 e garantire che siano legalmente vincolanti.	(b) prove sotto forma di sezioni di contratto con i fornitori che trattano i requisiti di questo regolamento.
7.3.3.	Il costruttore del veicolo ha individuato, valutato e trattato/gestito i rischi individuati, in maniera adeguata	Lo scopo di questo requisito è che i costruttori di veicoli identifichino gli elementi critici di un tipo di veicolo rispetto alla sicurezza informatica e giustificano le modalità di gestione dei rischi ad essi correlati. Il costruttore dovrebbe essere in grado di fornire una giustificazione del motivo per cui ha identificato elementi di un tipo di veicolo come critici (o meno). È opportuno sottolineare i seguenti chiarimenti (a) Gli elementi critici possono essere elementi che contribuiscono alla sicurezza del veicolo, alla protezione dell'ambiente o alla protezione dal furto. Possono essere parti che forniscono connettività. Possono anche essere parti dell'architettura del veicolo critiche per la condivisione di informazioni o per la sicurezza informatica (ad esempio, anche i gateway potrebbero essere considerati critici); (b) L'intento di questo requisito è quello di garantire che i rischi siano trattati/gestiti in modo appropriato prendendo in considerazione tutte le minacce, compreso l'allegato 5, parte A, e giudicando la necessità di contromisure in base ai risultati dell'analisi e della valutazione dei rischi; (c) L'intento di questo requisito è quello di consentire al costruttore del veicolo di dimostrare l'applicazione del processo pertinente ai requisiti 7.2.2.2. e 7.2.2.4. del CSMS al tipo di veicolo; (d) L'autorità di omologazione o il servizio tecnico devono fare riferimento all'allegato 5 del regolamento sulla sicurezza informatica per valutare la valutazione dei rischi del costruttore; (e) L'esame dei rischi deve tenere conto dei requisiti di cui al punto 7.3.4. e del requisito di attenuazione proporzionata; (f) La considerazione delle minacce e delle mitigazioni dell'Allegato 5 all'interno di una valutazione del rischio può portare a valutazioni come "non rilevante" o "rischi trascurabili".	Possono essere applicabili i seguenti standard: (g) ISO/SAE 21434 descrive il modo in cui definire il concetto. Questo include anche la considerazione di elementi critici basati su decisioni di trattamento del rischio. I risultati sono documentati in "[WP-09-03] Obiettivi di sicurezza informatica" e "[WP-09-06] Concetto di sicurezza informatica". La clausola 15 "Analisi delle minacce e metodi di valutazione del rischio" descrive inoltre la valutazione esaustiva del rischio. Ciò è documentato in "[WP-09-02] TARA"; (h) ETSI TS 103 645 può essere utilizzato per dimostrare la sicurezza degli elementi dell'Internet degli oggetti di un veicolo; (i) può essere utilizzata la norma BSI PAS 1885. Per comprovare questo requisito si può utilizzare quanto segue: (j) Il tipo di veicolo dichiarato; (k) Una spiegazione del perché gli elementi del tipo di veicolo sono critici; (l) Quali misure di sicurezza sono state implementate, comprese le informazioni sul loro funzionamento; (m) Le informazioni sulle misure di sicurezza devono consentire al Servizio Tecnico/Autorità di Omologazione di avere la certezza che tali misure rispondono alle intenzioni del costruttore e che i veicoli in produzione utilizzeranno le stesse misure presentate all'Autorità di Omologazione/Servizio Tecnico per il tipo di veicolo. La riservatezza delle informazioni specifiche e le modalità di gestione devono essere concordate e registrate.
7.3.4.	Il costruttore del veicolo ha protetto il tipo di veicolo dai rischi individuati nella sua valutazione del rischio	L'obiettivo di questo requisito è garantire che i costruttori di veicoli adottino misure di mitigazione appropriate in conformità con i risultati della loro valutazione del rischio. Il costruttore dovrebbe fornire argomentazioni e prove motivate per le attenuazioni che ha implementato nella progettazione del tipo di veicolo e perché sono sufficienti. Ciò può includere	Possono essere applicabili i seguenti standard: (d) ISO/SAE 21434 descrive la determinazione del rischio e gli obiettivi e il concetto di Cybersecurity dedotti sulla base dei rischi identificati. I risultati sono documentati in "[WP-09-03] Obiettivi di sicurezza informatica" e "[WP-09-06] Concetto di sicurezza informatica"; (e) La BSI PAS 11281: 2018 e altri standard relativi ad affermazioni, argomenti e prove possono essere utilizzati per giustificare le decisioni progettuali del produttore.

		qualsiasi ipotesi fatta, ad esempio sui sistemi esterni che interagiscono con il veicolo. Le attenuazioni tecniche di cui all'allegato 5, parti B e C, sono considerate ove applicabili ai rischi da mitigare. Il fabbricante può presentare una motivazione non solo per il fatto che una mitigazione elencata nell'allegato 5 sia "non pertinente o non sufficiente", ma può anche presentare una motivazione per cui un'altra mitigazione diversa da quelle elencate nell'allegato 5 è appropriata al rispettivo rischio. Tale motivazione può essere corroborata da una valutazione del rischio e da una classificazione del rischio che dimostri l'adeguatezza della mitigazione alternativa. Questo per consentire l'adozione di tecnologie difensive nuove o migliorate. Per architetture esistenti che sono state sviluppate prima che il Regolamento UN R155 entrasse in vigore, potrebbe non esser stato possibile sviluppare l'architettura in modo tale che tutte le misure di mitigazione elencate nell'Allegato 5, parti B e C fossero attuate. Pertanto, per omologazioni rilasciate per la prima volta prima del 1° luglio 2024, sono consentite altre misure di mitigazione di natura appropriata ai rischi di sicurezza informatica identificati. Ulteriori modifiche o aggiornamenti di natura tecnica che richiedano estensioni a questi tipi esistenti posteriormente al 1° luglio 2024 dovrebbero aderire il più possibile all'Allegato 5. Si dovrà fornire l'attenzione adeguata ai rischi e confermare che gli stessi continuano ad essere controllati o ridotti. Laddove vi siano scostamenti dall'Allegato 5 questi dovrebbero essere illustrati e giustificati. È opportuno sottolineare i seguenti chiarimenti: (a) Le decisioni di progettazione del produttore devono essere collegate alla valutazione del rischio e alla strategia di gestione del rischio. Il fabbricante deve essere in grado di giustificare la strategia attuata; (b) Il termine "proporzionato" deve essere considerato quando si sceglie se implementare una mitigazione e quale mitigazione implementare. Se il rischio è trascurabile, si può sostenere che una mitigazione non sia necessaria; (c) Protezione dai rischi identificati significa mitigare il rischio.	Per comprovare le mitigazioni utilizzate si possono utilizzare i seguenti elementi: (f) Prova che le misure di mitigazione sono state introdotte in base alla necessità delle misure, tra cui: (i) la ragione, se sono state applicate misure di mitigazione diverse da quelle dell'Allegato 5, parti B e C; (ii) il motivo per cui non sono state applicate le misure di mitigazione elencate nell'Allegato 5; (iii) il motivo, se le misure di mitigazione sono ritenute non necessarie.
7.3.5.	Il costruttore del veicolo ha messo in atto misure adeguate e proporzionate per garantire che (se previsti) sul tipo di veicolo siano presenti ambienti dedicati per conservare e far funzionare software, servizi, applicazioni o dati post-vendita	Vanno segnalati i seguenti chiarimenti: (a) Per "misure adeguate e proporzionate" si intende che il costruttore è in grado di giustificare le modalità di gestione dei rischi associati a qualsiasi ambiente dedicato, come definito nella valutazione dei rischi; (b) Gli ambienti dedicati possono trovarsi sul veicolo. Se il veicolo interagisce con server o servizi situati al di fuori del veicolo (ad esempio nel cloud), occorre considerare i rischi per il veicolo derivanti da questi ultimi, in relazione alla loro sicurezza informatica.	Possono essere applicabili i seguenti standard: (c) ISO/SAE 21434 descrive le fasi di elaborazione delle conclusioni per l'architettura. In "[WP-15-03] Scenari di minaccia" sono documentate le potenziali minacce alla conservazione e all'esecuzione di software, servizi, applicazioni o dati aftermarket. In "[WP-09-06] Concetto di sicurezza informatica" vengono descritte le misure appropriate e proporzionate. Per comprovare questo requisito si potrebbe utilizzare quanto segue: (d) Una descrizione dell'ambiente dedicato;

			(e) Quali misure di sicurezza sono implementate, comprese le informazioni sul loro funzionamento; (f) Le informazioni sulle misure di sicurezza devono consentire all'Autorità di omologazione/Servizio tecnico di avere la certezza che tali misure rispondono alle intenzioni del costruttore e che i veicoli in produzione utilizzeranno le stesse misure presentate all'Autorità di omologazione/Servizio tecnico per il tipo di veicolo. La riservatezza delle specifiche e le modalità di gestione devono essere concordate e registrate; (g) si deve fare riferimento all'allegato 5 del regolamento sulla sicurezza informatica.
7.3.6.	Il costruttore del veicolo ha effettuato, prima dell'omologazione, prove adeguate e sufficienti per verificare l'efficacia delle misure di sicurezza attuate	I risultati delle prove devono essere validi al momento dell'omologazione. Il Servizio Tecnico può eseguire test di sicurezza per confermare i risultati. È opportuno sottolineare il seguente chiarimento: (a) L'obiettivo di qualsiasi misura di sicurezza sarà quello di ridurre i rischi. I test devono giustificare le misure di sicurezza implementate.	Possono essere applicabili i seguenti standard: (b) I produttori possono descrivere le misure di verifica e convalida attuate in conformità alla norma ISO/SAE 21434 sotto forma di "[WP-10-07] Rapporto di integrazione e verifica", "[WP-11-01] Rapporto di convalida". Per comprovare questo requisito si può utilizzare quanto segue: (c) Cosa viene testato e perché (ad esempio, quali sono le misure di successo del test); (d) Metodologia utilizzata e perché (ad esempio, questo può includere note sull'estensione e sullo sforzo contenuto nei test); (e) Chi ha eseguito i test e perché (ad esempio, all'interno dell'azienda, un fornitore o un'organizzazione esterna e qualsiasi informazione pertinente sulla loro qualificazione/esperienza); (f) la conferma dell'esito positivo (che può includere i criteri di superamento/errore e il risultato del test).
7.3.7.	Il costruttore, per il tipo di veicolo in questione: a) ha rilevato e prevenuto gli attacchi informatici b) ha potenziato la sua capacità di monitoraggio c) dispone di capacità di trattamento dei dati che consentano di analizzare gli attacchi informatici	L'obiettivo di questo requisito è garantire che siano implementate misure specifiche per il tipo di veicolo per monitorare i cambiamenti nel panorama delle minacce, rilevare e prevenire gli attacchi informatici e avere la capacità di supportare in modo forense l'analisi di qualsiasi attacco tentato o riuscito. È opportuno notare i seguenti chiarimenti: (a) Le misure relative a questa clausola possono essere implementate sul tipo di veicolo o nel suo ambiente operativo, ad esempio il backend, la rete mobile "per il tipo di veicolo"; (b) Le misure devono mirare principalmente a prevenire gli attacchi informatici, con riferimento ai punti 7.3.4 e 7.3.5, per proteggere dai rischi identificati nella valutazione dei rischi; (c) Le misure per evitare che gli attacchi informatici abbiano successo contro tutti i veicoli di un tipo di veicolo possono anche essere fornite in modo asincrono, cioè dopo l'evento effettivo di un attacco informatico e la sua analisi; (d) La capacità di analisi forense dei dati può comprendere la capacità di fornire e analizzare i dati di registro, i codici di errore diagnostici, le informazioni operative del veicolo e le informazioni di backend per indagare sugli attacchi informatici; (e) la capacità di analisi forense dei dati può includere un buffer circolare di dati di log persistenti a supporto delle procedure investigative.	Possono essere applicabili i seguenti standard: (f) ISO/SAE 21434. L'identificazione delle fonti per il monitoraggio della sicurezza informatica è fornita in [RQ-08-01] e documentata in "[WP-08-01] Fonti di informazioni sulla sicurezza informatica". I risultati dell'analisi e le modalità di documentazione sono descritti in "[WP-08-05] Analisi delle vulnerabilità". Per comprovare questo requisito si può utilizzare quanto segue: (g) Misure di prevenzione degli attacchi applicate al tipo di veicolo; (h) Dimostrazione del funzionamento delle misure preventive e delle attività di monitoraggio di un tipo di veicolo; (i) Dimostrazione di come viene eseguita l'analisi forense.

		Si noti che il paragrafo 1.3. e la conformità alle leggi sulla privacy dei dati è particolarmente rilevante per questo requisito.	
7.3.8.	I moduli crittografici utilizzati ai fini del presente regolamento sono in linea con le norme concordate Se i moduli crittografici utilizzati non sono in linea con le norme concordate, il costruttore del veicolo ne ha giustificato l'uso	È opportuno notare i seguenti chiarimenti: Una norma concordata potrebbe essere una norma riconosciuta a livello internazionale o una norma nazionale di uso comune, ad esempio FIPS. L'intento di questo requisito è garantire che i metodi di crittografia utilizzati possano essere giustificati.	Quando vengono implementate misure di crittografia, sulla base dei risultati dell'analisi e della valutazione dei rischi, il produttore deve essere in grado di: (a) spiegare se l'algoritmo o la misura di crittografia sono conformi a uno standard di consenso attuale; e (b) spiegare il motivo della scelta della crittografia e perché riduce adeguatamente il rischio individuato.

Tabella 12 – Lista di riscontro per la valutazione di tipo

7.2 VERIFICHE TECNICHE E PROVE

Nel corso della valutazione di tipo del veicolo, il Servizio Tecnico acquisirà gli elementi utili alla definizione di un piano per la ripetizione di alcune prove fisiche sul veicolo campione atte a dimostrare l'efficacia delle misure di mitigazione adottate dal Costruttore in risposta alle minacce individuate.

Il Servizio Tecnico deciderà quali prove ripetere sotto la propria supervisione presso il Costruttore o presso un laboratorio accreditato e ne valuterà l'esito redigendo un apposito verbale di prova.

La decisione su quali prove debbano essere ripetute sarà basata sull'esame della valutazione dei rischi e sui risultati delle prove già effettuate dal Costruttore o da laboratori accreditati nella fase di sviluppo del tipo di veicolo. Il Servizio Tecnico presterà particolare attenzione all'elenco dei rischi, delle minacce e delle misure di mitigazione elencate nell'Allegato 5 del Reg. UN R155.

ALLEGATO 1

ESEMPIO DI STRUTTURA DELLA MATRICE DI CONFORMITÀ
[Paragrafi 7.2.2.2.(b) e 7.2.2.2.(c) del Reg. UN R155]

Esempio

7.2.2.2. ll costruttore del veicolo deve dimostrare che i processi utilizzati nell'ambito del suo sistema di gestione della cybersicurezza garantiscono che la sicurezza sia stata adeguatamente presa in considerazione, anche in relazione ai rischi e alle misure di attenuazione elencati nell'allegato 5. Tali processi devono includere: b) i processi utilizzati per l'identificazione dei rischi per i tipi di veicolo. Nell'ambito di tali processi devono essere prese in considerazione le minacce di cui all'allegato 5, parte A, e altre minacce pertinenti;	Lo scopo di questo requisito è che il costruttore dimostri che i processi, le procedure utilizzate per identificare i rischi dei tipi di veicolo. I processi implementati dovrebbero considerare tutte le probabili fonti di rischio. Questo includerà i rischi identificati nell'allegato 5 del regolamento sulla cybersicurezza. Es. I rischi che derivano dai servizi di connessione o dipendenze esterne. Le fonti per l'identificazione del rischio possono essere dichiarate. Queste possono includere: (a) Vulnerabilità/minacce da piattaforme condivise; (b) Lezioni apprese circa rischi e vulnerabilità.	Questo requisito è coperto dai processi descritti in: • §8-Panoramica della metodologia della valutazione del rischio • §10-Analisi delle minacce e della valutazione del rischio (TARA) • §11-Trattamento del rischio
7.2.2.2. ll costruttore del veicolo deve dimostrare che i processi utilizzati nell'ambito del suo sistema di gestione della cybersicurezza garantiscono che la sicurezza sia stata adeguatamente presa in considerazione, anche in relazione ai rischi e alle misure di attenuazione elencati nell'allegato 5. Tali processi devono includere: c) i processi utilizzati per la valutazione, la categorizzazione e il trattamento dei rischi individuati;	Lo scopo di questo requisito è che il costruttore dimostri il processo e le regole che usa per la valutazione, la categorizzazione e l'identificazione dei rischi da minacce.	Questo requisito è coperto dai processi descritti in: • §8-Panoramica della metodologia della valutazione del rischio • §10-Analisi delle minacce e della valutazione del rischio (TARA) • §11-Trattamento del rischio

ALLEGATO 2

MODELLO DI ISTANZA PER LA CERTIFICAZIONE DEL CSMS
[Paragrafo 6.2. del Reg. UN R155]

(°)

Al Ministero delle Infrastrutture
e della Mobilità Sostenibili
Dipartimento per la mobilità sostenibile
Direzione Generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione
Divisione 3

Oggetto: Richiesta di verifica del sistema di gestione della sicurezza informatica (CSMS) ai fini del rilascio della certificazione ai sensi del Regolamento UN R155

Subject: Request for Cybersecurity Management System (CSMS) assessment aimed at certification issue in compliance with UN Regulation No. 155

Il sottoscritto / *The undersigned*		
In qualità di / *In my capacity of*		(*)
del Costruttore / *of the OEM*		
con sede in / *based in*		
email / *email*		
rivolge istanza affinché per lo/gli stabilimento/i sito/i in *makes an application in order to, for the plant/plants based in*		

a) sia verificata l'idoneità del CSMS / *assess the CSMS compliance* ☐

b) sia confermata l'idoneità del CSMS / *confirm the CSMS compliance* ☐

A tal fine dichiara che il Costruttore presso il suindicato stabilimento produce:
For this purpose I declare that the OEM at the above mentioned plant/plants manufactures:

☐ Veicoli / *Vehicles* _____ (**)

Al riguardo allega alla presente richiesta i seguenti documenti (+):
To this extent the following documents are attached to the application (+):

- Attestazione dei versamenti previsti: CCP 9001 di euro 10,20 e CCP 4028 di euro 32.00;
  Receipt of the requested payments
- Estremi della Camera di commercio o documento equivalente per Stati esteri;
  References of the Chamber of Commerce or equivalent document for foreign Countries
- Descrizione sintetica della produzione svolta nel sito per il quale si chiede l'ispezione;
  General description of the current operations for the plant/plants covered by the application
- Descrizione del sistema di gestione della sicurezza informatica per il sito per il quale si chiede l'ispezione;
  Description of the cyber security management system for the plant/plants covered by the application
- Certificazioni ISO e/o di altri Stati membri ove presenti;
  ISO certificates and/or certificates granted by other Type Approval Authorities, if existing
- Copia della domanda di omologazione presentata (nel caso di avvio della produzione);
  Copy of the type approval application (in the case of start of production)
- Accordo nel caso di produzione presso un sito di altro Costruttore.
  Signed agreement in the case of production taking place at another OEM's plant

Si resta in attesa delle decisioni da parte della Commissione per la valutazione del CSMS di codesto ufficio.
Waiting for the decisions taken by the Commission being charged of the CSMS audit

Luogo, data
Place, date _____

Firma (***)
Signature

_____

Note:
Notes:

(°) Costruttore: utilizzare carta intestata della ditta
OEM: use the letterhead of the Manufacturer

(*) titolare, amministratore delegato, rappresentante legale, mandatario o persona legalmente autorizzata o delegata alla firma delle istanze e alla effettuazione di dichiarazioni vincolanti per il Costruttore.
owner, CEO, legal representative, emissary or person legally authorised or designated to sign the application and to make declarations that are binding for the OEM

(**) indicare la tipologia dei veicoli, dei dispositivi prodotti e la relativa categoria internazionale o nazionale (es. autovetture, autocarri, autobus, trattori. ecc.).
specify the type of vehicles and the relevant International or National category (e.g. passenger cars, commercial vehicles, buses, tractors, etc…)

(***) timbro della ditta, nome e qualifica del firmatario. Allegare documento di riconoscimento del firmatario.
seal of the manufacturer, name and position of the undersigned (ID card of the undersigned is attached)

(+) documentazione obbligatoria.
mandatory documentation

Istruzioni per la compilazione: riportare le informazioni nei campi grigi
Instructions: provide the requested information by filling-in the grey fields

ALLEGATO 3

MODELLO D'ISTANZA DI OMOLOGAZIONE DEL TIPO DI VEICOLO

[Paragrafo 3.1. del Reg. UN R155]

Al Ministero delle infrastrutture e della mobilità sostenibili

Dipartimento per la mobilità sostenibile

Direzione Generale …

Servizio Tecnico (esplicitare) …

Il sottoscritto / *The undersigned*

……

in qualità di **(1)**:
*in my capacity of **(1)**:*

□ legale rappresentante / *legal representative*

□ rappresentante accreditato presso il Centro Prova Autoveicoli di / *representative accredited to the Technical Service of* ……..

□ mandatario (se ricorre) / *emissary (if applicable)*

……..

del costruttore / *of the OEM*

……..

con sede legale in / *with registered office in*

……..

e sito produttivo / *and manufacturing plant*……..

rivolge istanza affinché il veicolo (categoria)
makes an application so that the following vehicle (category)
.....)
(2)(3):

Marca (denominazione commerciale) / *Make (brand name)*..... **(4)**

nel tipo di seguito indicato, possa ottenere, ai sensi della seguente normativa **(5)**:
*of the following type be granted, with reference to the following regulation **(5)**:*

.....…….…….…….…….…….…….…….…….…….…….…….…….…….…

L'OMOLOGAZIONE / ESTENSIONE / AGGIORNAMENTO / REVISIONE DELL'OMOLOGAZIONE **(6)**:
*THE TYPE APPROVAL / AN EXTENSION / AN UPDATE / A REVISION OF THE TYPE APPROVAL **(6)**:*

TIPO **(7)** *TYPE **(7)***	N° MARCHE OPERATIVE **(8)** *N° OF TAX STAMP **(8)***	DATA VERSAMENTO *DATE OF DEPOSIT*	CODICE TARIFFA **(9)** *TARIFF CODE **(9)***
……..	……..…	……	……..…

DICHIARAZIONI
DECLARATIONS

Si dichiara che per la stessa omologazione:
I hereby declare that for the same approval:

a) non è stata presentata analoga domanda presso un altro Stato membro/altro Paese contraente dell'Accordo internazionale di Ginevra **(10)** o presso altro Centro Prova Autoveicoli;
*no other application was made to a different Member State/Contracting Party of the '58 Agreement **(10)** or to another Technical Service*

b) nessuna autorità di omologazione ha rifiutato di rilasciare un'omologazione del tipo in questione;
no other Type Approval Authority has refused to grant the approval for the relevant type

c) nessuna autorità di omologazione ha revocato l'omologazione del tipo in questione;
no other Type Approval Authority has withdrawn the approval for the relevant type

d) non è stata revocata la domanda di omologazione per il tipo in questione.
the application for approval of the relevant type has not been rejected

La documentazione tecnica prevista (scheda informativa ed elaborati tecnici) è allegata e/o verrà perfezionata nell'ambito delle verifiche e prove. **(11)**
*The requested technical documentation (communication file and technical papers) is attached and/or will be produced during the relevant assessment and testing **(11)***

Sono stati assolti i previsti oneri stabiliti dalla normativa vigente secondo la voce tariffaria ~~6~~ della tabella 3 della legge 01/12/1986 n. 870 con pagamento tramite PagoPA secondo il tariffario individuabile al seguente link
Duties specified by the legislation in force have been fulfilled in compliance with the tariff code 6 under table 3 of Law 01/12/1986 n. 870 through a deposit with PagoPA following the price list available at the following link
https://www.ilportaledellautomobilista.it/web/portale-automobilista/pagamenti-pagopa.

Si fa presente che i prototipi necessari per le verifiche e prove sono già disponibili/sono disponibili
The prototypes needed for the relevant assessment and testing are already available/will be available

Dal / *from* ……..**(12).**

Le verifiche e prove si svolgeranno presso il sito produttivo/laboratorio
Assessment and testing will be performed at the following plant/laboratory
……..……..……..……..……...**(13)**

Data e Luogo
Date and Place

Firma del richiedente **(14)**
*Signature of the applicant **(14)***

……..

……

……

Note:
Notes:

(1) Contrassegnare la voce che ricorre
Tick as applicable

(2) Depennare i casi che non ricorrono
Strikeout the items which do not apply

(3) Per i veicoli e i sistemi indicare la categoria secondo quanto previsto dal Codice della Strada dagli artt. 52-60 e/o dal regolamento UE/UNECE, ove ricorre
For vehicles and systems specify the category as specified by the Road Traffic Law (articles 52 to 60) and/or by the EU/UNECE regulation, if applicable

(4) Se ricorre indicare la marca del prodotto
If applicable specify the brand name

(5) Indicare la norma che si intende applicare (Regolamento UNECE, Regolamento UE, Norma nazionale, altro):
Specify the applicable regulation (UN Regulation, EU Regulation, National Standard, other)

a) Per il Regolamento UNECE, indicare il numero del Regolamento, l'emendamento e il supplemento
In case of a UN Regulation, specify the number, series of amendments and supplement

b) Per il regolamento UE, indicare il Regolamento base e l'ultimo regolamento di modifica (se esistente)
In case of a EU Regulation, specify the base Regulation and the latest amendment available (if existing)

c) Per la normativa nazionale, indicare l'articolo del Codice/Regolamento o il DM pertinente con anche, se prevista, la norma CUNA/ISO di riferimento
In case of a National Standard, specify the Law/Regulation article or the relevant Decree together with the reference CUNA/ISO standard if applicable

(6) Depennare i casi che non ricorrono. In caso di estensione/aggiornamento/revisione completare con gli estremi di omologazione
Strikeout the items which do not apply. In case of extension/update/revision also provide the type approval details

(7) Ove ricorrano varianti e versioni, allegare una tabella nella quale siano specificate le differenze che determinano l'introduzione di varianti/versioni ai fini tariffari
Where variants and versions are foreseen, provide (for tariff purposes) a table to highlight the differences which demand for the introduction of such variants/versions

(8) Da completare a cura del Centro Prova Autoveicoli
To be completed by the Technical Service

(9) Indicare uno o più dei codici previsti dalla tabella 3 legge 870/86
List one or more codes as foreseen by table 3 of Law 870/86

(10) Depennare i casi che non ricorrono
Strikeout the items which do not apply

(11) Inserire elenco allegati
Enter the list of attachments

(12) Barrare la voce che non ricorre e indicare, se ricorre, la data di disponibilità
Strikeout the item that does not apply and specify the availability date, if applicable

(13) Da completare con la denominazione, se esistente, del laboratorio (la denominazione/indicazione con la sede è obbligatoria se trattasi di Ente terzo). Indicare in ogni caso se il laboratorio è/non è certificato ISO 17025 e fornire, in caso positivo, gli estremi di certificazione ISO 17025 n° ……..
To be completed with the name of the laboratory, if applicable (the name and address is requested in case of a third party lab). Specify in any case if the laboratory is/is not ISO 17025 accredited and, in the affirmative, provide the accreditation number n°…….

(14) Indicare in stampatello per esteso nome, cognome e qualifica di chi firma (come designato dal costruttore e depositato presso il CPA) ovvero – in caso di mandatario - far seguire con le parole "per conto di"
Specify in block letters and in full the first name, family name and position of the applicant (as identified by the OEM and registered at the Technical Service) or, in the case of an emissary, complete with the words "on behalf of"

ALLEGATO 4

MODELLO DI VERBALE DI VALUTAZIONE DEL SISTEMA CSMS

Ministero delle Infrastrutture e della Mobilità Sostenibili

Dipartimento per la mobilità sostenibile

Direzione generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione

Divisione 3

VERBALE n° *AUDIT N.*	DEL *DATE*

Conformità al Sistema di Gestione della Cybersicurezza (CSMS)
Compliance with the Cyber Security Management System (CSMS)

Verifica delle specifiche del costruttore al Punto 7. del Regolamento ECE N. 155
Verification of the manufacturer's specifications at Point 7. of ECE Regulation No. 155

COSTRUTTORE / *MANUFACTURER*

Denominazione _____

Name _____

Sede legale _____

Registered Office _____

Mandatario in Italia _____

Mandatary in Italy _____

Stabilimenti di produzione _____

Production plant(s) _____

_____

_____

Categorie di veicoli per le quali il Costruttore richiede Audit triennale di processo
Vehicle categories for which the manufacturer requires triennial process Audits

☐ M _____

	N	

PREMESSA / *PREMISE*

Il costruttore dichiara di aver adottato tutte le misure necessarie a ottemperare agli obblighi sul sistema di gestione della cybersicurezza (CSMS). *The manufacturer declares that it has taken all necessary measures to comply with the requirements for the cybersecurity management system (CSMS).*	**Sì / Yes**	**No**

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

1 CARATTERISTICHE GENERALI DELL'ORGANIZZAZIONE PRODUTTIVA *GENERAL CHARACTERISTICS OF THE PRODUCTIVE ORGANIZATION*

1.1	Il Costruttore ha predisposto un'organizzazione aziendale, responsabilità e ambiti di competenza del personale addetto, risorse e misure opportune, piani di controllo documentati, istruzioni per l'esecuzione dei test, gestione dei report, verifica dei risultati e controllo del piano per verificare che il sistema di gestione della cybersicurezza (CSMS) sia conforme al regolamento. *The Manufacturer has in place a business organization, responsibilities and areas of responsibility of relevant personnel, appropriate resources and measures, documented control plans, test execution instructions, report management, results verification, and plan control to verify that the cybersecurity management system (CSMS) is in compliance with the regulation.*	**2**	**1**	**0**

DATA DELLA PRECEDENTE CERTIFICAZIONE _____
PREVIOUS CERTIFICATION DATE

N.ro DELLA PRECEDENTE CERTIFICAZIONE _____
PREVIOUS CERTIFICATION N.

0 = assenza totale del requisito / *total absence of the requirement*
1 = soddisfacimento parziale (necessarie azioni di miglioramento) / *partial satisfaction (necessary improvement actions)*
2 = soddisfacimento totale / *total satisfaction*

2 Verifica preliminare del Sistema di Gestione della Cybersicurezza (CSMS) *Preliminary verification of the Cybersecurity Management System (CSMS)*

7.1 - Reg. ECE N. 155

7.1.1	Il costruttore del veicolo dispone di processi che verificano che le prescrizioni del presente regolamento non limitano le disposizioni o le prescrizioni di altri regolamenti ONU.	**2**	**1**	**0**

	The vehicle manufacturer has processes that verify that the requirements of this Regulation shall not restrict provisions or requirements of other UN regulations.			
FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*				

3 Controllo della conformità del Sistema di Gestione della Cybersicurezza (CSMS) *Cybersecurity Management System (CSMS) Compliance Monitoring*				
7.2 del Regolamento ECE N. 155				
7.2.2.1.	Il costruttore del veicolo dispone di un sistema di gestione della cybersicurezza che si applica alle seguenti fasi: (a) fase di sviluppo, (b) fase di produzione, (c) fase di post-produzione. *The vehicle manufacturer has a Cyber Security Management System which applies to the following phases: (a) development phase, (b) production phase, (c) post-production phase.*	**2**	**1**	**0**
7.2.2.2.(a)	Il costruttore dispone di processi all'interno della propria organizzazione per gestire la cybersicurezza. *The vehicle manufacturer has processes used within the manufacturer's organization to manage cyber security.*	**2**	**1**	**0**
7.2.2.2.(b)	Il costruttore dispone di processi utilizzati per l'identificazione dei rischi per i tipi di veicolo; nell'ambito di tali processi prende in considerazione le minacce di cui all'Allegato 5, Parte A del Regolamento e altre minacce pertinenti. *The vehicle manufacturer has processes used for the identification of risks to vehicle types; within these processes, the threats in Annex 5, Part A of the Regulation and other relevant threats are considered.*	**2**	**1**	**0**
7.2.2.2.(c)	Il costruttore dispone di processi utilizzati per la valutazione, la categorizzazione e il trattamento dei rischi individuati. *The vehicle manufacturer has processes used for the assessment, categorization and treatment of the risks identified.*	**2**	**1**	**0**
7.2.2.2.(d)	Il costruttore dispone di processi per verificare che i rischi individuati siano gestiti in modo adeguato. *The vehicle manufacturer has processes in place to verify that the risks identified are appropriately managed.*	**2**	**1**	**0**
7.2.2.2.(e)	Il costruttore dispone di processi utilizzati per testare la cybersicurezza di un tipo di veicolo. *The vehicle manufacturer has processes used for testing the cyber security of a vehicle type.*	**2**	**1**	**0**
7.2.2.2.(f)	Il costruttore dispone di processi utilizzati per garantire che la valutazione del rischio sia mantenuta aggiornata. *The vehicle manufacturer has processes used for ensuring that the risk assessment is kept current.*	**2**	**1**	**0**
7.2.2.2.(g)	Il costruttore dispone di processi utilizzati per monitorare, individuare e rispondere agli attacchi e minacce informatiche e alle vulnerabilità dei tipi di veicolo e di processi	**2**	**1**	**0**

	utilizzati per valutare se le misure di cybersicurezza attuate siano ancora efficaci alla luce delle nuove minacce informatiche e vulnerabilità individuate. *The vehicle manufacturer has processes used to monitor for, detect and respond to cyberattacks, 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.*	
7.2.2.2.(h)	Il costruttore dispone di processi utilizzati per fornire dati pertinenti a sostegno dell'analisi di attacchi informatici tentati o riusciti. *The vehicle manufacturer has processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.*	**2** **1** **0**
7.2.2.3.	Il costruttore dispone di processi utilizzati nel suo sistema di gestione della cybersicurezza che, sulla base della categorizzazione riferite ai commI (c) e (g) del punto 7.2.2.2, garantiranno che le minacce informatiche e le vulnerabilità siano attenuate entro un lasso di tempo ragionevole. *The vehicle manufacturer has processes used within their Cyber Security Management System that ensure that, based on categorization referred to paragraphs 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.*	**2** **1** **0**
7.2.2.4.	Il costruttore dispone di processi utilizzati all'interno del proprio sistema di gestione della cybersicurezza che garantiscono che il monitoraggio riferito al comma (g) del punto 7.2.2.2. sia continuo, includa i veicoli dopo la prima immatricolazione e sia capace di analizzare e rilevare minacce informatiche, vulnerabilità e attacchi attraverso i dati e i log dei veicoli. *The vehicle manufacturer has processes used within their Cyber Security Management System that ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual, include vehicles after first registration and is capable to analyse and detect cyber threats, vulnerabilities and cyberattacks from vehicle data and vehicle logs.*	**2** **1** **0**
7.2.2.5.	Il costruttore ha dimostrato in che modo il suo sistema di gestione della cybersicurezza gestirà le eventuali dipendenze con fornitori, fornitori di servizi o sub-organizzazioni del costruttore per quanto riguarda le prescrizioni riferite al punto 7.2.2.2.. *The vehicle manufacturer has demonstrated 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.*	**2** **1** **0**
FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*		

NUMERO DI RISPOSTE / *NUMBER OF RESPONSES*	
NUMERO DI "ZERO" (N) / *NUMBER OF "ZERO" (N)*	
SE I TEST SONO STATI EFFETTUATI DA SOCIETA' ESTERNA AL COSTRUTTORE SI ATTRIBUISCE UN PUNTO ADDIZIONALE / *IF THE TESTS WERE CARRIED OUT BY COMPANY OUTSIDE THE MANUFACTURER AN ADDITIONAL POINT IS AWARDED*	

TOTALE PUNTEGGIO / *TOTAL SCORE*	

MEDIA OTTENUTA (M) / *AVERAGE OBTAINED (M)* TOTALE PUNTEGGIO ÷ NUMERO DI RISPOSTE / *TOTAL SCORE ÷ NUMBER OF ANSWERS*	

Il numero di risposte è riferito a quelle applicabili al costruttore e viene utilizzato per il calcolo del punteggio finale

The number of responses refers to those applicable to the constructor and is used to calculate the final score

OSSERVAZIONI / *OBSERVATIONS*

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

NOTA / *NOTE*

Le valutazioni si basano su tre livelli: / *Evaluations are based on three level* :

2 – esiste ed è operante; / *it exists and is operational*;
1 – esiste ma incompleto/non documentato ma operante/operante saltuariamente; / *t exists but incomplete/undocumented but operating/operating occasionally*;
0 – non esiste/inoperante. / *does not exist/operates*.

A conclusione della stesura del presente verbale di verifica la valutazione finale del Costruttore sarà:

At the conclusion of the preparation of this Verification Report, the OEM's final evaluation will be:

DI IDONEITA' se sono verificate entrambe le condizioni seguenti: / ***ELIGIBLE*** *if both of the following conditions are met*:

- assenza di "ZERO": / *absence of "ZERO":* **N=0**
- media M ottenuta: / *average M obtained*: **1,7 ≤ M**

DI IDONEITA' CON RISERVA se sono verificate entrambe le condizioni seguenti: / ***ELIGIBLE WITH RESERVATION*** *if both of the following conditions are met*:

- assenza di "ZERO": / *absence of "ZERO":* **N=0**
- media M ottenuta: / *average M obtained*: **1,4 ≤ M < 1,7**

DI NON IDONEITA' se si verifica anche solo una delle seguenti condizioni: / ***NOT ELIGIBLE*** *if only one of the following condition is met*:

- numero di "ZERO": / *number of "ZERO":* **N > 0**
- media M ottenuta: / *average M obtained*: **M < 1,4**

VALUTAZIONE FINALE / *FINAL EVALUATION*

In esito a quanto riportato sul presente verbale,
According to the final evaluation reported in this audit,

SI RITIENE / *IS CONSIDERED*

che il costruttore indicato in epigrafe, presso i locali soggetti a sopralluogo ha illustrato le proprie misure del sistema di gestione della cybersicurezza (CSMS) in conformità al regolamento ECE N. 155 con valutazione finale:
that the manufacturer named in the epigraph, at the premises subject to inspection, has illustrated its cybersecurity management system (CSMS) measures in accordance with ECE Regulation No. 155 with the final evaluation:

IDONEA
ELIGIBLE ☐

IDONEA CON RISERVA
ELIGIBLE WITH RESERVATION ☐

NON IDONEA
NOT ELIGIBLE ☐

e si trasmette il presente verbale per le determinazioni conseguenti.
and this audit is transmitted for the consequent determinations.

Luogo e data del sopralluogo / *Place and date of inspection*

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

Nome	Cognome	Ufficio di appartenenza *Office of affiliation*
Name	*Surname*	
		D.G. MOT. - DIV. 3
		D.G. MOT. - DIV. 3

ALLEGATO 5

MODELLO DI VERBALE DI VISITA E PROVA DEL TIPO DI VEICOLO

Ministero delle Infrastrutture e della Mobilità Sostenibili

Dipartimento per la mobilità sostenibile

Direzione Generale …….

Servizio Tecnico (esplicitare) …

-

Rapporto di prova n° _____- *Test report no.*

Relativo alle verifiche e prove per l'omologazione dei veicoli per quanto concerne la cyber sicurezza e al sistema di gestione della cyber sicurezza - Regolamento UNECE N. 155. *Related to checks and tests for EEC type approvals with regard regards to cyber security and cyber-security management system- UNECE Regulation No. 155*

Marca: *Make:*	XXXX op./or XXXX
Tipo e denominazione commerciale del veicolo: *Type and trade name of manufacturer:*	XXXXXXXXXXX
Veicoli appartenenti allo stesso tipo ai sensi del punto 2.1.: *Vehicles belonging to the same type under of point 2.1.:*	Vedere schemi n° XXXX *see scheme no….*
Categoria del veicolo: *Category of the vehicle:*	XX

Nome e indirizzo del costruttore: *Name and address of manufacturer:*	XXXXXXXXXXX
Caratteristiche del veicolo: *Vehicle characteristics:*	vedere scheda informativa */see information document* XXXXXXXX
Data della domanda: *Application request date:*	00/00/0000
Luogo e data delle verifiche e prove: *Place and date of checks and tests:*	Torino, 00/00/0000
Nome e indirizzo del laboratorio di prove: *Name and address of the test laboratory:*	--

PREMESSA / *INTRODUCTON*

- L'atto normativo di cui all'oggetto, prevede un modello di verbale di prova: **NO**

  A standard test report was provided in the regulatory act mentioned in the subject: ***NO***

PROVE / *TEST*

- Il costruttore e l'autorità di omologazione o il servizio tecnico hanno identificato una configurazione peggiore da sottoporre a prova rappresentativa di tutte le configurazioni? **SI/NO/N.A.**
  The manufacturer and the type-approval authority or technical service have identified a worst-case configuration, to test that configuration as representatives of all the configurations? ***YES/NO/N.A.***

- Informazioni relative al modo in cui è stata trovata la configurazione peggiore del sistema, del componente o dell'entità tecnica indipendente: **SI/NO/N.A.**
  Information about how the worst-case system, component or independent technical unit configuration was found: ***YES/NO/N.A.***

- Sono stati utilizzati metodi di prova diversi da quelli prescritti negli atti normativi applicabili e da essi consentiti? **SI/NO/N.A.**
  Other test methods than those prescribed in the applicable regulatory acts and by them permitted had been used? ***YES/NO/N.A.***

- Descrizione dei metodi utilizzati e consentiti diversi da quelli prescritti negli atti normativi applicabili: **SI/NO/N.A.**
  Description of test methods used and different than those prescribed in the applicable regulatory acts: ***YES/NO/N.A.***

- Campionamento: **SI/NO/N.A.**
  *Sampling****: YES/NO/N.A.***

a) identificazione dei veicoli, del sistema, del componente o dell'entità tecnica indipendente sottoposto/a a prova: **SI/NO/N.A.**

identification of the vehicle, system, component or separate technical unit tested: ***YES/NO/N.A.***

b) descrizione dettagliata delle caratteristiche del veicolo, del sistema, del componente o dell'entità tecnica indipendente prescritte dall'atto normativo applicabile di cui all'allegato II del regolamento (UE) 2018/858:

detailed description of the vehicle, system, component or separate technical unit characteristics required by the applicable regulatory act listed in Annex II to Regulation (EU) 2018/858:

- vedere scheda informativa n. XXXXXXXX.

- see information document no. XXXXXXXX.

c) risultati delle verifiche prescritte stabiliti dall'atto normativo applicabile: vedi tabella successiva ed allegati

results of the prescribed checks required by the applicable regulatory act: see next table and annex

Sul veicolo/prototipo presentato alle prove sono stati condotti i seguenti accertamenti:

On the prototype vehicle under examination, have been verified as listed below:

7.3	Prescrizioni per i tipi di veicolo / *Requirements for vehicle types*		
7.3.1	Il costruttore è in possesso di un certificato di conformità valido* per il sistema di gestione della cibersicurezza relativo al tipo di veicolo da omologare. *Per le omologazioni anteriori al 10 luglio 2024, Il costruttore dimostra che il veicolo non è stato sviluppato in maniera conforme al CSMS, e dimostra che la cibersicurezza è stata presa in considerazione durante la fase di sviluppo del tipo di veicolo in questione. *The manufacturer has a valid Certificate of Compliance* for the Cyber Security Management System relevant to the vehicle type being approved.* ** For approvals prior to 1 July 2024, the manufacturer demostrate that vehicle type could not be developed in compliance with the CSMS and shows that cybersecurity was adequately considered during the development phase of the vehicle type concerned.*		2 1 0 - vedi Certificato di conformità per il CSMS allegato* - see c*ertificate of Compliance for the CSMS annex** *Vedi allegato XXYY per le omologazioni anteriori al 10 luglio 2024 **See annex XXYY for approvals prior to 1 July 2024*
7.3.2	Il costruttore del veicolo ha individuato e gestito, per il tipo di veicolo da omologare, i rischi connessi ai fornitori. *The vehicle manufacturer has identified and managed, for the vehicle type concerned, supplier-related risks.*		2 1 0 Vedi allegato XXYY *See annex XXYY*
7.3.3	Il costruttore del veicolo ha individuato, valutato e trattato/gestito i rischi individuati, in maniera adeguata. *The vehicle manufacturer has identified, performed an exhaustive risk assessment and treated / managed the risks identified appropriately.*		2 1 0 Vedi allegato XXYY (rif. allegato 5, parte A) *See annex XXYY (ref. Annex 5, Part A)*
7.3.4	Il costruttore del veicolo ha protetto il tipo di veicolo dai rischi individuati nella sua valutazione del rischio. *The vehicle manufacturer has protected the vehicle type against risks identified in the vehicle manufacturer's risk assessment.*		2 1 0 Vedi allegato XXYY (rif.allegato 5, parte B-C) *See annex XXYY (ref. Annex 5, Part B-C)*
7.3.5	Il costruttore del veicolo ha messo in atto misure adeguate e proporzionate per garantire che (se previsti) sul tipo di veicolo siano presenti ambienti dedicati per conservare e far funzionare di software, servizi, applicazioni o dati post-vendita. *The vehicle manufacturer has 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.*		2 1 0 Vedi allegato XXYY *See annex XXYY*
7.3.6	Il costruttore del veicolo ha effettuato, prima dell'omologazione, prove adeguate e sufficienti per verificare l'efficacia delle misure di sicurezza attuate. *The vehicle manufacturer has performed, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.*		2 1 0 Vedi allegato XXYY *See annex XXYY*
7.3.7	Il costruttore, per il tipo di veicolo in questione: a) ha rilevato e prevenuto gli attacchi informatici; b) ha potenziato la sua capacità di monitoraggio; c) dispone di capacità di trattamento dei dati che consentano di analizzare gli attacchi informatici. *The vehicle manufacturer, for the vehicle type:* *(a) has detected and prevented cyber-attacks;* *(b) has supported the monitoring capability;* *(c) provides data forensic capability to enable analysis of attempted or successful cyber-attacks.*		2 1 0 Vedi allegato XXYY *See annex XXYY*
7.3.8	I moduli crittografici utilizzati ai fini del presente regolamento sono in linea con le norme concordate. Se i moduli crittografici utilizzati non sono in linea con le norme concordate, il costruttore del veicolo ne ha giustificato l'uso.		2 1 0

	Cryptographic modules used for the purpose of this Regulation are in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer has justified their use.		Vedi allegato XXYY *See annex XXYY*
	Totale punteggio / T*otal score*		
	Media / *Average*		

Criteri di valutazione/ Evaluation criteria

Le valutazioni si basano su tre livelli: / *Evaluations are based on three level :*
2 – esiste ed è operante; / *it exists and is operational;*
1 – esiste ma incompleto/non documentato ma operante/operante saltuariamente; / *it exists but incomplete/undocumented but operating/operating occasionally;*
0 – non esiste/inoperante. / *does not exist/operates*.

A conclusione della stesura del presente verbale di verifica la valutazione finale del Costruttore sarà:
At the conclusion of the preparation of this Verification Report, the Builder's final evaluation will be:

DI IDONEITA' se sono verificate entrambe le condizioni seguenti: / *ELIGIBLE if both of the following conditions are met:*
- assenza di "ZERO": / *absence of "ZERO":* N=0
- media M ottenuta: / *average M obtained:* $1,7 \leq M \leq 2$

DI NON IDONEITA' se si verifica anche solo una delle seguenti condizioni: / *NOT ELIGIBLE if only of the following condition is met:*
- numero di "ZERO": / *number of "ZERO":* $N > 0$
- media M ottenuta: / *average M obtained:* $M < 1,7$

d) La quantità delle fotografie scattate durante le prove è a discrezione dell'autorità di omologazione. Nelle prove virtuali, le fotografie possono essere sostituite da stampe di schermate o altri elementi probanti adeguati: **SI/NO/N.A.**

The number of photographs taken during the tests at the discretion of the approval authority. In virtual tests, photographs they may be replaced by prints of screens or other appropriate external evidence: ***YES/NO/N.A.***

OSSERVAZIONI / *OBSERVATIONS* ***N.D.***

CONCLUSIONI E PARERI / ***CONCLUSIONS AND OPINIONS***

- Conclusioni generali delle prove per il sistema, il componente o l'entità tecnica indipendente sottoposto a prova e rappresentativo/a del tipo da omologare:
  O*verall test conclusions for the system, component or separate technical unit in the test report that was representative in terms of the type to be approved:*

  Sulla base dei criteri di valutazione stabiliti, i veicoli sono conformi alle prescrizioni della norma richiamata in oggetto.

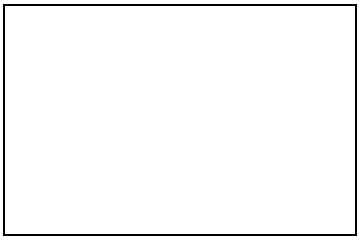
  Based on the established evaluation criteria , the vehicles are comply with the requirements of the provision referred to in item.

- Pareri o interpretazioni inclusi in questo verbale di prova.
  Opinions and interpretations included in this test report.

Rapporto di prova concluso il **00/00/0000**.
Test report concluded on

IL FUNZIONARIO DEL SERVIZIO TECNICO

(dott. ing. _____)



VISTO
IL DIRETTORE DEL DERVIZIO TECNICO

(dott. ing. _____)