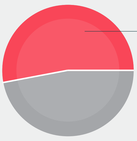
CYBERSECURITY LIFECYCLE MANAGEMENT FOR MODERN VEHICLES IS A COMPLEX PROCESS.

AUTOSEC HELPS SAVE TIME AND RESOURCES.

Where the industry stands - assessing the current approach to cybersecurity lifecycle management



Over

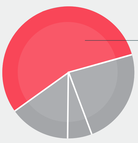
50%

of automotive professionals testify that **they do not have traceability.**

*According to C2A's research.

Without complete visibility, cyber resilience becomes a near impossible task. We asked OEMs and Tier 1s if they have traceability from software and hardware BOM to VIN; **over half of them do not.**

The faster a Threat Analysis and Risk Assessment (TARA) test can be run, the faster improvements can be but in place. However, over half (56%) of respondents say the risk assessment process **takes more than three weeks to manage.**

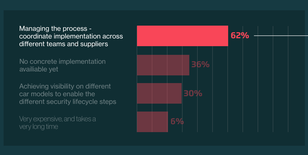


56%

say that the risk assessment process **takes more than three weeks to manage.**

*According to C2A's research.

ISO 21434 IMPLEMENTATION - WHAT'S YOUR CHALLENGE?

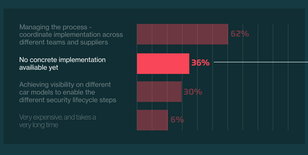


62%

ranked **coordinated implementation across different teams and suppliers** as the #1 challenge

*According to C2A's research.

To effectively adopt ISO 21434 regulation, teams must implement a more methodical, systematic approach to cybersecurity across all organizations. However, 62% of respondents ranked coordination across different teams and suppliers as the #1 challenge to ISO 21434 implementation.

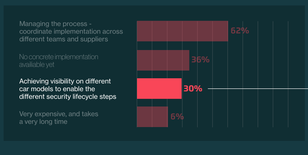


36%

Ranked **the lack of concrete implementation steps available**

*According to C2A's research.

No clear guidance on how to shift to regulation-compliance could distract from building streamlined cybersecurity practices. 36% of security practitioners ranked this as their core challenge to ISO implementation.



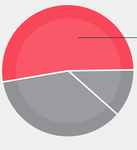
30%

Rank **visibility over different car models throughout the security lifecycle steps** as a core challenge

*According to C2A's research.

Full spectrum visibility is critical for the successful implementation of ISO 21434. However, 30% of automotive leaders rank visibility over different vehicle models as a main inhibitor to adoption.

DIVING INTO THE DETAIL - RISK ASSESSMENT TODAY



Over

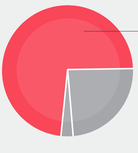
50%

Rank **coordination between different entities** is the #1 impediment

*According to C2A's research.

The foundation of any timely risk assessment project: communication is key. **Stakeholders rank this as the number one impediment to speedy TARA processes.**

As the industry shifts, so must who takes responsibility for risk assessment. **70% believe responsibility should be split equally among parties, by each entity down the supply chain.**



Over

70%

believe that risk assessment process should be managed **by each entity down the supply chain.**

*According to C2A's research.

AutoSec

Provides scalable, efficient protection throughout the vehicle lifecycle.

ANALYSIS | NETWORK | ENDPOINT | ATTACKER

Designed to meet automotive relevant, industry specific needs, AutoSec is a comprehensive Cyber Security Management System (CSMS) for the entire vehicle lifecycle. Seamlessly integrated with any existing suite of cybersecurity solutions or external modules, its intuitive design empowers industry stakeholders to identify and mitigate cyber risks in today's challenging environment. Threat Analysis and Risk Assessment (TARA), in-vehicle protection, vulnerability analysis and validation are easily managed through the AutoSec platform. Only when armed with AutoSec can cybersecurity teams effectively collaborate, delegate security work across the entire supply chain and design in-vehicle protection.

c2a-sec.com info@c2a-sec.com