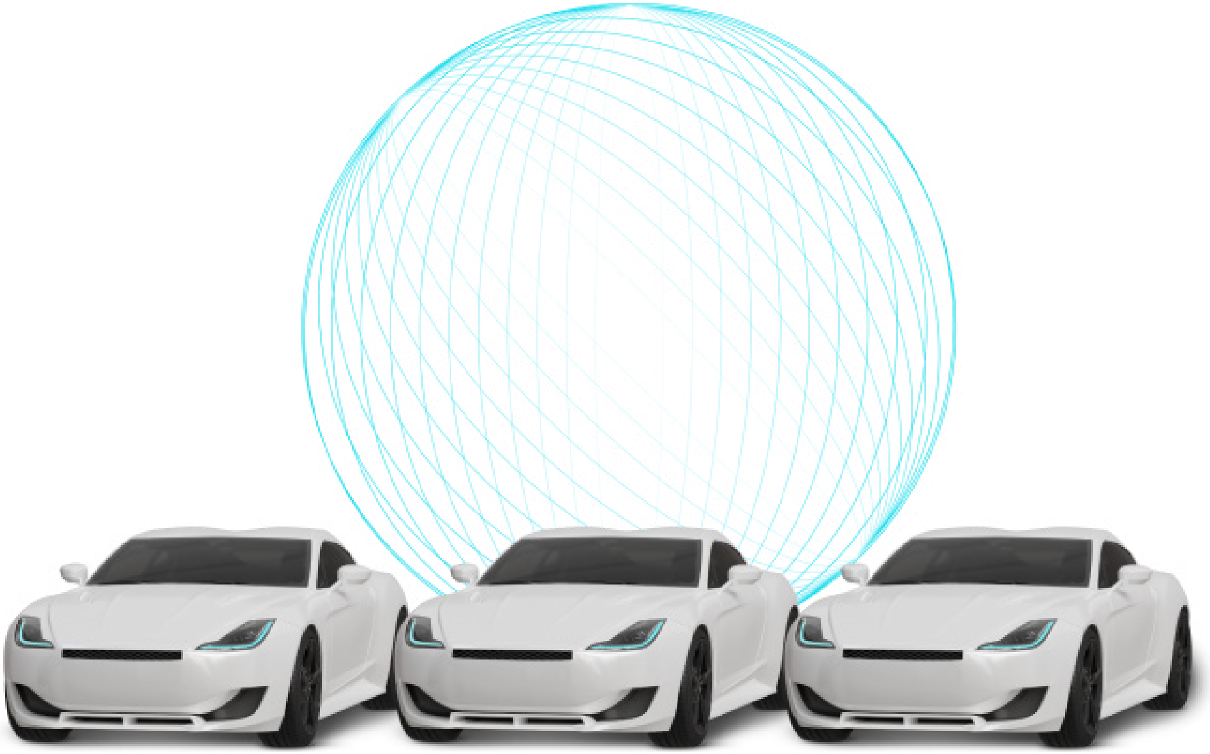
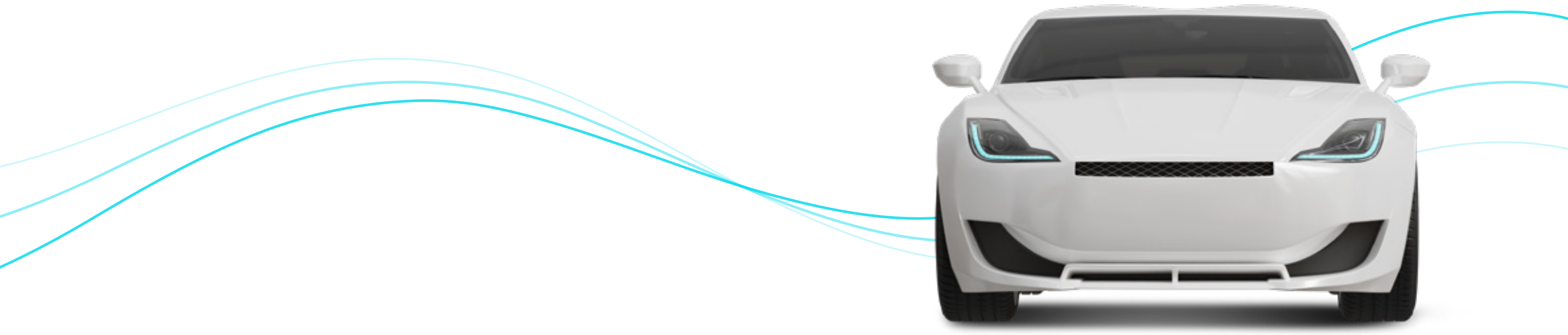
ARGUS Continental

Streamlining Automotive Cyber Security Management

CSMS Implementation Approach for UNR 155 Compliance



Content



Background

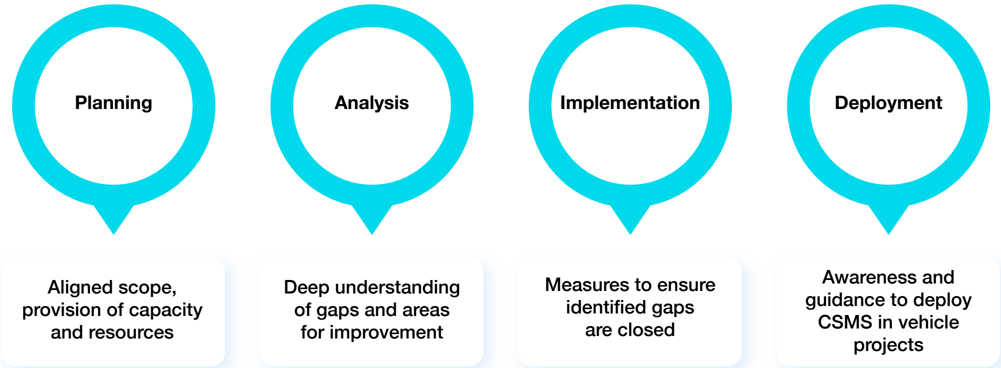
The UNR155 automotive cyber security regulation which came into effect in July 2022, mandates vehicle manufacturers (OEMs) to demonstrate a risk-based management framework (also known as a Cyber Security Management System or CSMS) for discovering, analyzing, and protecting against relevant threats, vulnerabilities, and cyber attacks. The processes used by the OEM to do this must be applied to the development, production, and post-production stages of the vehicle lifecycle. By following UNR155, each OEM must obtain a CSMS "certificate of compliance" (CoC) before its vehicles are eligible to be considered for type approval.

In response to these new requirements and the related business and lifestyle opportunities presented by connectivity and software, over the last few years, Argus has been ramping up its work with OEMs on the development of necessary cyber-risk management processes. To accelerate this service offering and create a wider net of available competencies and resources, Argus has come together with Continental Business Consulting to meet the growing demand of automotive-grade cyber security, functionality safety and quality management expertise.

In this paper, we will share an approach used to successfully implement a cyber security management system for an established OEM. The approach and the insights within are based on a real-world project where Argus and Continental experts reviewed and improved cyber security management processes of the OEM for achieving a CSMS certificate of compliance (CoC) recognized by UNECE/WP.29 type approval authorities.

The approach

An implementation approach for CSMS within an organization is influenced by a variety of internal and external factors, such as allocated resources and the maturity of existing engineering processes. These factors naturally act as important inputs for the project effort estimation. Therefore, the CSMS implementation journey should begin by assigning clear roles and responsibilities (to individuals sourced from existing or adjacent domains and external supporting resources) to achieve the implementation goals. The implementation journey can generally be split into the following phases:



Planning

Aligned scope, provision of capacity and resources

Analysis

Deep understanding of gaps and areas for improvement

Implementation

Measures to ensure identified gaps are closed

Deployment

Awareness and guidance to deploy CSMS in vehicle projects

Planning

Typically, such an implementation project begins by aligning the internal process owners and stakeholders with respect to the scope, expectations, and outcome of the planned phases within the project. Some of the key topics to address during the planning phase are listed below:

- Assign a dedicated resource that oversees and coordinates all the implementation activities
- Identify relevant stakeholders for the different processes, functional areas, etc
- Plan for the required resources throughout the project according to organizational capacity
- Follow frameworks such as SIPOC (Suppliers, Inputs, Process, Outputs and Customers) and RASI (Responsible, Accountable, Supporting, Informed)
- Keep end process stakeholders in mind for ensuring process usability in projects (e.g., the needs of TARA engineers)
- Implement suitable training and process piloting to achieve maturity in small steps

In all cases, a clear overview of organizational capabilities should be maintained – the cyber security transformation project is not meant to “reinvent the wheel” but to have a repeatable, increasingly effective CSMS which fits into the overall process and improvement cycles within the company. This phase is very decisive for the project success as it needs proper frontloading and due consideration to risks and limitations. The effort for this phase can vary depending on the organization. From our experience, this has been the most time-consuming phase running into months due to the need to find and allocate resources, reach consensus and alignment with a variety of stakeholders etc.

Gap Analysis

One of the first tasks in this phase is to gain a clear picture of the existing process landscape. Such an effort can ensure:

- Mapping and understanding existing organizational and development processes
- Aligning of planned or ongoing CSMS implementation activities, if any

The initial analysis can be performed through an offline review of the processes in place and then inviting the relevant stakeholders (i.e., process owners) for a deep-dive into their processes. During these sessions, the stakeholders verify weaknesses, gaps or non-compliance with regulatory requirements. For normative baselining, our experts advise clients to use resources such as the VDA ACSMS, the UNR155 interpretation document and aspects of ASPICE.

During sessions with process owners, it is essential to critically review the existing CSMS processes, how they interact with other product development and organizational processes, which roles are involved, etc. For example, when analyzing supplier management processes, it is important to verify that cyber security considerations are covered in activities like supplier qualification, selection and monitoring.

Another focus area is to identify missing process interfaces and dependencies. With proper planning in the beginning, this phase can be concluded relatively quickly (within 2-5 weeks); including all sessions, post-session documentation and results consolidation activities.

Ratings

All identified gaps, once documented, should be weighted to provide a rating. Through this rating, the process owners get an understanding of the gap(s) between existing processes and what is required for compliance with the applicable normative baseline(s). Adhering to the rating schemes in VDA ASCMS and ISO/PAS 5112 is recommended.

Stakeholder workshop

Conducting a joint workshop with all process owners and key process stakeholders is crucial. In this workshop, improvement measures with a precise “definition of done” (DOD) should be defined based on the rating of identified gaps. This helps the project team to ensure that the expected deliverables are clear, prioritized, estimated, assigned and scheduled for implementation with all the relevant personnel.

Implementation

Once the improvement measures are available by the end of the Analysis phase, the **Implementation Phase** can begin. During this phase, the process owners define and perform their implementation tasks using the DOD as a guiding principle. In typical consulting projects, Argus and Continental supports the project team by guiding process owners in defining and planning their implementation tasks, performing alignment workshops with the relevant stakeholder etc.

For Argus and Continental, the role of a “guide” primarily means supporting process owners to understand dependencies, confront questions and challenges, brainstorm, review next steps and generally help them navigate their domain towards an optimal solution. This way of working ensures that internal resources are imbued with the skills to take full, independent ownership of the tasks at hand with minimal external support.

During the implementation phase, the project team can also rely on and orient themselves through detailed (albeit generic) process guidance documents and work product templates. These documents clearly outline the process flow, input, and output relations between process activities and work products as well as the key requirements that must be fulfilled by the work product (e.g., test entry and exit criteria in a test plan). Through generic process guidance documents (provided by Argus or otherwise aligned with industry best practices), many benefits can be realized (e.g., an advanced starting point, reduced menial task work, better understanding of prerequisites, etc.), especially in process areas that have low maturity or did not exist at all.

As the implementation tasks are completed and processes are defined, Argus and Continental recommend a delta analysis to verify whether identified gaps or non-conformities have been fixed. From an effort point of view this phase can run over several months. We recommend our clients to conclude the implementation tasks between 3 - 6 months. This however depends on the scope of work, availability of resources and organizational complexity etc.

Deployment

The final phase of CSMS implementation (excluding the formal process of applying for a CoC) is **Deployment**. In this phase, the organization must ensure that it has the levels of awareness, know-how and support required to launch vehicle projects within the framework of a fully functional CSMS. In this deployment phase, special attention should be given to the collection of end-user experiences and feedback. This is to make sure that continuous improvements are achieved for CSMS operations as well as efficiencies and general competence. Argus and Continental recommend providing adequate support to the project team during the deployment phase to support the fulfillment of process requirements. Such support may come, for instance, in the form of subject-matter experts participating in work product reviews.

Summing it all up

As the complexity of automotive cyber security regulations continues to grow, achieving compliance requires a deep and comprehensive understanding of automotive processes, cyber security know-how and proven compliance experience. As described above, Argus and Continental have developed a proven methodology for CSMS implementation, including gap analysis, process definition, deployment and ongoing support, to assist vehicle manufacturers in minimizing their cyber risk and meet UN R155 regulatory requirements for vehicle type approval.

Argus Consulting & Engineering

Built by Argus and Continental Business Consulting on a foundation of knowledge and contributions from Continental’s Product Cyber Security community of automotive safety, quality and security experts, Argus Consulting & Engineering enables automotive manufacturers and suppliers to achieve automotive-grade cybersecurity for automotive components, vehicles and management systems. With Argus Consulting & Engineering, you are plugging into cyber security and automotive expertise to prepare mobility for the security challenges of a software-defined world.