Compliance (https://www.cyeqt.com/en/category/compliance-en/)

Regulations & Standards (https://www.cyeqt.com/en/category/regulations-standards-en/)

UN R155 Audit: Checklist and tools for preparing for the CSMS audit

Manuel Sandler · 31. July 2024

During an audit in accordance with UN Regulation No. 155 (UN R155 for short) or UN R155 audit / CSMS audit, a vehicle manufacturer is faced with the task of proving its Cyber Security Management System (CSMS for short). According to UN R155, this involves two main steps. The first step is an audit at organizational level, in which implemented processes are assessed and which is not tied to specific products. The second step is a product-specific evaluation, the so-called product assessment. Although UN R155 has only applied to the type approval of all new vehicles since July 2024, there are already best practices and recommendations for carrying out UN R155 audits.

Manuel Sandler

Furthermore, a number of players in the industry, both OEMs and suppliers, but also auditing institutions, are still unsure about the measures and benchmarks required for an audit. There is uncertainty about the expectations of the auditors, the level of detail required and the exact scope of the audit. Those responsible at organizational and project level are often unclear as to whether

their approach can be considered appropriate or whether they have perhaps even proceeded in too much detail/overdimensioned. In addition, there is a great need for information on the part of the companies as to what questions the auditors will ask and how they can be adequately prepared for them.

(https://www.cyeqt.com/)

As UN Regulation No. 155 in its full scope of application along the entire value chain (and for neighboring vehicle industries besides the automobile) is still quite new, there are only a few widely known industry insights around the UN R155 audit. Companies carrying out the audit for the first time often have no reference.

Nevertheless, there are tools and checklists that can help companies to prepare. These tools can be used to determine whether the measures taken are sufficient and logically coherent, which contributes significantly to passing the audit.

The following is an up-to-date look at existing checklists and tools.

KBA checklist for the UN R155 audit

An initial aid is a checklist published by the German Federal Motor Transport Authority (Kraftfahrt-Bundesmamt, short KBA). The Federal Motor Transport Authority (KBA) has created a catalog with minimum requirements for preparing for an audit for UN R155 as well as for UN R156. The catalog combines questions and requirements for both Cybersecurity Management Systems (CSMS) and Software Update Management Systems (SUMS). It is freely available on the KBA website in German and English.

The approach here is that each question within the catalog refers to requirements that can be derived from the two regulations. In this way, the catalog offers companies the opportunity to check exactly whether they meet the necessary requirements before an audit. The statement of compliance with the requirements should also include an explanation of the methods and evidence used.

However, there is no reference to ISO/SAE 21434 in this catalog.

The catalog is divided into various sections, whereby general requirements for CSMS and SUMS are discussed first. This is followed by risk management requirements, process requirements and other requirements in accordance

with UNR 156. Topics such as monitoring and measurement are also covered.

The focus of the questions is on risk management. However, some of the questions in the German version in particular are difficult to understand, which is why it is advantageous to already be familiar with the terminology of UN R155 and UN R156. In addition to the specific requirements for these two subject areas, there is a section with general requirements for a management system, which are fundamental for both cybersecurity and software updates.

Tip for beginners: Discover our video learning course on ***UN Regulation No 156 + Software Update Management System (SUMS): A Comprehensive Guide for Automotive Professionals*** (https://base.cyeqt.com/course/un-regulation-156-software-update-management-system-guide-automotive-video)

LEARNING ADVICE

Advantages and disadvantages of the KBA catalog for UN R155/UN R156

The main advantage of the KBA catalog is firstly that it was created directly by an approval authority, i.e. by the body that ultimately decides what is to be expected. Furthermore, it is the only one of the three checklists presented here that combines the CSMS with the SUMS. Accordingly, reference is made to the requirements of UN R155 and UN R156 for each requirement. It is also very helpful to differentiate where concrete evidence is required and where requirements can be covered by pure process descriptions. The KBA catalog is also the only one that explicitly requires and lists non-cybersecurity-specific requirements as a basis. These are also very helpful for the initial development of a CSMS, as they allow the necessary QMS basics to be checked.

In addition to the positive aspects, however, it should be noted that the terminology used, particularly in the German version, has already led to confusion in practice at various companies.

The requirements also overlap in some cases, so that the catalog is anything but self-explanatory the first time it is used.

It is also important to mention that the KBA catalog is based exclusively on the UN regulations and does not take ISO/SAE 21434 or other relevant norms and standards into account to any significant extent.

Accordingly, it should only be used to prepare for a UN 155/156 audit and not for an ISO/SAE 21434 audit. It is therefore primarily only of interest to OEMs and not to suppliers. Finally, it should be mentioned that the KBA catalog is primarily used by the German KBA in cooperation with various TÜV institutions and is therefore not (yet) internationally established.

VDA Automotive Cybersecurity Management System Audit

The second checklist we are looking at comes from the German Association of the Automotive Industry (Verband der Deutschen Automobilindustrie, short VDA) and its Quality Management Center (QMC). It is entitled “Automotive Cyber Security Management System Audit”. The approach is similar to that of the KBA.

The checklist includes general requirements and definitions for a Cyber Security Management System. This includes requirements for auditors, the process flow, an evaluation system (for each question and for the overall result) and, above all, a questionnaire.

This questionnaire is divided into nine main topics:

1. cyber security management
2. risk identification
3. risk assessment and categorization
4. consistency check
5. cyber security specification
6. verification, validation and release
7. update of the risk assessment
8. incident response and reporting to authorities
9. cyber security management in the supply chain

There are questions and associated minimum requirements for each topic. These are based on both UNR 155 and ISO/SAE 21434, but without direct reference to the specific requirement IDs in the official document of the standard or regulation.

(https://catalog.cyber-cs.com/)

The catalog can be used analogously by looking at questions and minimum requirements and using evidence to show how your own Cyber Security Management System meets them.

It is important to note that the catalog refers exclusively to a Cyber Security Management System and not to Software Update Management. There is also a guide for auditors and a glossary.

In contrast to the KBA catalog, however, this is subject to a charge.

Advantages and disadvantages of the VDA Automotive CSMS audit catalog (“Red Book”)

The level of detail in the VDA document represents a good mix of technical depth and clarity. As already mentioned, it also contains further in-depth information on the audit, which can also be helpful for the general implementation of internal audits.

The proposed assessment scheme also ensures a uniform assessment. As it uses aspects of both the standard and the regulation, it can be used for the preparation of both an ISO/SAE 21434 audit and a UN R155 audit.

On the other hand, it should be noted that this publication has since been officially withdrawn by the VDA. The reasons for this are not entirely transparent to the public, but reference is made to other existing standards. Another disadvantage is that the document was primarily known on the German market and received little international attention. The fact that the document was subject to a charge was also a reason why many companies did not use it.

ENX Vehicle Cybersecurity (VCS) Audit Scheme

Finally, we look at the ENX Association's Vehicle Cyber Security Audit Scheme to see how it can support a UN R155 audit. The ENX, known for TISAX, recognized the high demand for ISO/SAE 21434 certification and the resulting challenge that certification results are difficult to compare, especially in an international context and given the numerous accredited certification bodies. This was one of the starting points for the development of a standardized framework for industry-specific cybersecurity audits.

A project group developed a detailed catalog based on various standards and regulations. The aim was to create a uniform assessment scheme for cybersecurity.

The result is an Excel file that is now freely available on the ENX website.

Compared to the KBA catalog and the VDA audit, this scheme is much more comprehensive. It looks at cybersecurity holistically and not just in isolation in relation to regulations. It aims to make companies and products more secure and not just to pass audits quickly and easily.

The inputs for the Vehicle Audit Scheme include ISO/SAE 21434, UN R155 and other standards. These include the VDA's *Control Questions* on Information Security Assessments and excerpts from ISO 19011. *ISO PAS 5112 Road Vehicles Guidelines for Auditing Cyber Security Engineering* is also used. A VDA position paper on the Development Interface Agreement and other VDA papers are also included. The VDA Automotive Cyber Security Management System Audit is also part of the scheme.

The audit catalog is divided into various main topics:

- Organizational cybersecurity, human resources incl. cybersecurity culture, risk management, internal assessments, concept and product development phase, post-development phase (excluding operations maintenance), operation security, incident management and supply chain.

For each chapter, there are questions with objectives and requirements that are either mandatory or optional. There is also additional information, recommendations and examples as well as a list of possible evidence to support companies.

Overall, the catalog is very extensive with almost 100 different requirements, spread over around 20 to 25 questions, whereby the requirements always refer to the corresponding requirements in the regulations/standard.

(https://www.cyeqt.com/en/)

Advantages and disadvantages of the ENX Vehicle Cybersecurity (VCS) Audit Scheme for cybersecurity audits

Compared to other catalogs, the ENX Audit Scheme is much more comprehensive and considers cybersecurity as a whole. Another advantage is that, in addition to ISO/SAE 21434, reference is made to various standards, including specific links to the corresponding requirements.

It can therefore be used both to prepare for a UN R155 audit and for audits in accordance with ISO/SAE 21434.

In addition to the requirements, the catalog also contains examples and recommendations so that even experienced cybersecurity managers can benefit and learn.

It is also important to mention the practical perspective: various companies from the industry (both on the manufacturer and supplier side) were involved in its creation. The document therefore covers different perspectives of the industry.

Perhaps it’s a matter of personal preference whether you prefer a minimal or comprehensive approach – the ENX catalog definitely takes a comprehensive approach, which can be overloaded and therefore overwhelming for smaller companies.

In fact, the catalog is extensive and may be too complex for smaller organizations. It is aimed more at larger companies with many developers and corresponding processes than at small manufacturers of niche products.

Nevertheless, the knowledge imparted is very helpful for anyone dealing with a Cyber Security Management System or an audit. It is therefore highly recommended that practitioners review the catalog and, if necessary, reduce it for their own context instead of excluding it from the very beginning.

The catalog is freely available and is based on current standards and regulations, which also speaks for its use. However, it is much more complex to edit than the KBA catalog.

- OEMs are required to have their implemented Cyber Security Management System (CSMS) audited **every three years** in accordance with UN Regulation No. 155. This is done at both the organisational/process level and the product assessment level.
- This will apply to the type approval of all new vehicles since **July 2024**. Those responsible at organisational and project level are often unsure of the exact expectations and requirements of the auditors.
- **Aids and checklists can help prepare for the audit,** such as the UN R155 audit checklist from the German Federal Motor Transport Authority, the VDA Automotive CSMS Audit Catalogue (no longer available) or the Vehicle Cyber Security Audit Scheme from the ENX Association, known for TISAX.
- The selection of an appropriate catalogue depends on the objectives, resources and circumstances of your own organisation - in any case, it is advisable to critically examine the consistency and robustness of your own procedures **prior to an audit.**

KEY LEARNINGS

(https://www.cyeqt.com/en/)

Conclusion on checklists for UN R155 audits

The choice of the appropriate catalog as a checklist for a UN R155 audit ultimately depends on the framework conditions of your own company and the objective of the exercise. For companies whose primary goal is to obtain the Certificate of Compliance with limited resources, the KBA catalog is recommended. If cybersecurity is to be addressed in the long term and as comprehensively as possible, the ENX scheme is certainly recommended. The VDA document is a good middle ground in between, but should be seen more as an internal tool and less for the exchange with the technical service or the approval authority due to its withdrawn publication.

Regardless of which catalog you choose, it is strongly recommended that you answer and justify each individual requirement in writing for the UN R155 audit.

In any case, this approach makes it possible to get to the bottom of the given challenges and to check both the consistency and the robustness of one's own approach vis-à-vis a potential auditor.

(https://www.cyeqt.com/en/)

This is the success criterion for passing a UN R155 audit, not the checklist used.

Tags:

Expert Tips & Best Practice (https://www.cyeqt.com/en/tag/expert-tips-best-practice-en/), Insights & Interpretation (https://www.cyeqt.com/en/tag/insights-interpretation-en/)

Share the Post:

Manuel Sandler

(https://www.cyeqt.com/en/)

Manuel Sandler is a globally recognized expert in automotive cybersecurity. As an independent consultant, he advises vehicle manufacturers and suppliers on cybersecurity strategies and implementation. As a knowledge management advisor for CYEQT Knowledge Base, he continues to work on improving the competency development programs and educational offerings that he has been involved in developing from the very beginning. With degrees in mathematics, Sandler has worked with renowned automotive organizations and global Tier-1 suppliers. He was a partner at CYRES Consulting, a leading consultancy in automotive cybersecurity. Sandler is also an author and sought-after speaker in the field.

Up to date bleiben? Newsletter abonnieren

Kostenlos | Relevanter Input zur Cybersecurity in der Fahrzeugentwicklung | Nicht zu häufig

Ihr Name

Unternehmen

Position

More resources and insights to strengthen your industry know how

(https://www.cyeqt.com/en/autonomous-driving-vs-cybersecurity/)

Autonomous driving vs. cybersecurity: Security as a key factor for the future of autonomous vehicles (https://www.cyeqt.com/en/autonomous-driving-vs-cybersecurity/)

Autonomous vehicles and cybersecurity: Technologies, risks, attack vectors & global regulations – your complete guide. Featuring key insights and best practices.

Read More (Https://Www.Cyeqt.Com/En/Autonomous-Driving-Vs-Cybersecurity/)

(https://www.cyeqt.com/en/)

(https://www.cyeqt.com/en/un-r155-worldwide-how-countries-regulate-vehicle-cybersecurity-in-2025/)

A look at the counterparts to UN Regulation No 155: Overview of global automotive cybersecurity regulation (mid-2025) (https://www.cyeqt.com/en/un-r155-worldwide-how-countries-regulate-vehicle-cybersecurity-in-2025/)

Global cybersecurity regulations in the automotive sector, including timelines and country-specific approaches in China, India, UK, South Korea & more.

Read More (Https://Www.Cyeqt.Com/En/Un-R155-Worldwide-How-Countries-Regulate-Vehicle-Cybersecurity-In-2025/)

(https://www.cyeqt.com/en/cyber-resilience-act-cra-in-the-automotive-industry/)

The Cyber Resilience Act (CRA) in the automotive industry: What carmakers and suppliers need to know (https://www.cyeqt.com/en/cyber-resilience-act-cra-in-the-automotive-industry/)

Cyber Resilience Act (CRA) is transforming automotive cybersecurity. How the EU regulation affects OEMs, suppliers and vehicle components – and what to do now.

(https://www.cyeqt.com/en/)

Read More (Https://Www.Cyeqt.Com/En/Cyber-Resilience-Act-Cra-In-The-Automotive-Industry/)

Your e-mail address to stay up to date

SUBSCRIBE →

CYEQT Knowledge Base offers unique, practical training opportunities and resources for sustainable competence development in automotive cybersecurity.

(https://www.linkedin.com/company/cyeqt)

RESOURCES

Automotive Cybersecurity Training (https://www.cyeqt.com/en/automotive-cybersecurity-training/)

Automotive Cybersecurity Courses Video (https://www.cyeqt.com/en/automotive-cybersecurity-video-courses/)

Automotive Cybersecurity Certification (https://www.cyeqt.com/en/automotive-cybersecurity-certification/)

ISO/SAE 21434 Templates(https://www.cyeqt.com/en/iso-sae-21434-templates/)

Automotive Cybersecurity Specialist Literature (https://www.cyeqt.com/en/automotive-cybersecurity-specialist-literature/)

→ Knowledge Hub(https://www.cyeqt.com/en/knowledge-hub/)

COLLABORATE

Advisory & Engineering Services (https://www.cyeqt.com/en/automotive-cybersecurity-advisory-engineering-services/)

(https://www.cyeqt.com/en/)

Call for Authors(https://www.cyeqt.com/en/call-for-authors/)

Partner Program(https://www.cyeqt.com/en/partner-program/)

CYEQT

About us(https://www.cyeqt.com/en/about-us/)

Expert Network(https://www.cyeqt.com/en/expert-network/)

Events(https://www.cyeqt.com/en/events/)

Careers(https://www.cyeqt.com/en/careers/)

Contact(https://www.cyeqt.com/en/contact/)