PG VCS Project Report

Frankfurt | October 2023

www.enx.com

Table of Contents

- Executive Summary
- Motivation
- Objective & Approach
- Organization of Project
- Results – Development and piloting of audit scheme
- Recommendations


“The audit was comprehensive. The auditors were experts, the audits probed deep into the CSMS, the results are reliable and transparent”

Executive Summary

Situation

- Appropriate risk management and governance necessary in the „entire supply chain“ for sustainable implementation of vehicle cybersecurity (VCS) over its lifecycle
- High demand for proprietary „ISO/SAE 21434“ certification schemes due to a lack of a standard scheme
- The project was set up to determine the feasibility of standardized audits for VCS of suppliers within ENX’s framework

Project Result

- CSMS auditing of suppliers within the ENX framework is a standardized, transparent way to realize reliable and comparable audit results
- Testing the developed VCS audit scheme confirms its feasibility
- Pilot audits demonstrated the maturity and effectiveness of the VCS scheme
- Version 1 of the VCS catalogue based on the learnings from the piloting audits is released

Recommendations

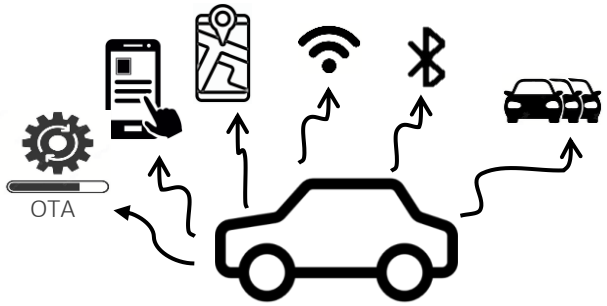
- ENX to provide the project results to the automotive cybersecurity community for further reviewing, commenting and use
- ENX to make the developed, piloted and revised VCS audit available to interested parties and to recognize the results gained during piloting
- Establish an ENX industry expert working group responsible for continuous support and improvement of the VCS scheme

Table of Contents

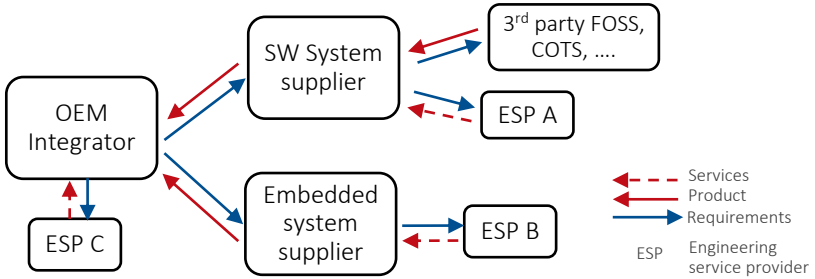
- Executive Summary
- Motivation
- Objective & Approach
- Organization of Project
- Results – Development and piloting of audit scheme
- Recommendations

Motivation

Situation in the automotive industry



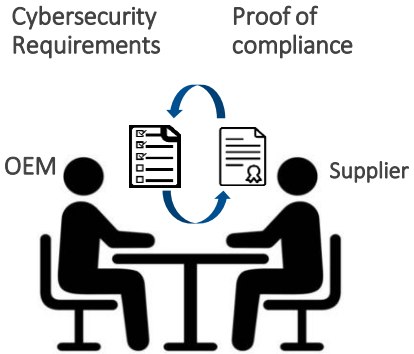
Vehicle digitalization:
The increasing digitalization of vehicle systems due to automated driving, connectivity and new mobility concepts necessitates management of vehicle cybersecurity



Supply chain complexity:
Bulk of the value addition and core competitiveness in the vehicle supply chain arise from suppliers of „software systems". Hence, threat and damage scenarios arising from unresolved cybersecurity risks must be appropriately managed along the supply chain

Cybersecurity Management System:
UNECE R-155 regulation mandates all OEMs to provide evidence of successful audit of the organization's CSMS in the form of a „Certificate of Compliance" CoC

Managing supplier dependencies



Supplier CSMS Audit:
Achieve and sustain security objectives, reduce compliance efforts and costs for customers and suppliers alike

Motivation

Background

- High demand for „ISO/SAE 21434“ certification
- No standard certification scheme exists
- Several proprietary certification schemes are on offer
- The industry has widely adopted certification of information security management systems of the automotive supply chain through ENX’s TISAX scheme
- Demand to study/prepare the utilization of TISAX framework for assessing CSMS of the supply chain
- Raised through individual stakeholders and executing a decision of the ENX Board, a project was set up

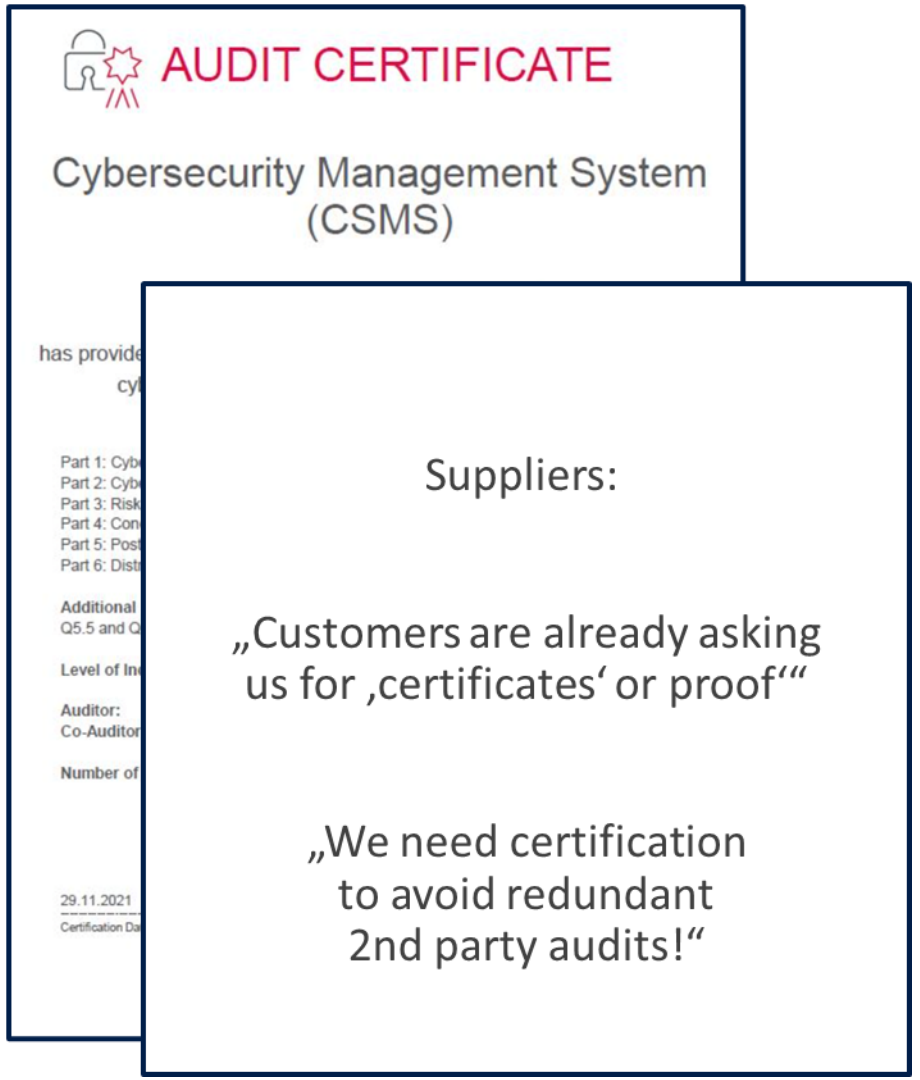


Table of Contents

- Executive Summary
- Motivation
- Objective & Approach
- Organization of Project
- Results – Development and piloting of audit scheme
- Recommendations

Objective

Determine the feasibility of executing VCS Audits for suppliers within the TISAX Framework

Approach

Initial questions - How should VCS audits look like?

- What is the nature of interaction between the audit provider and the audit participant?
  - Self-assessment by supplier
  - Audit by customer (second-party)
  - Neutral, objective audit of implementation of criteria as per defined procedure (third-party)
- The ISO/SAE 21434, which is primarily an engineering standard, can be used to derive criteria for a process certification as well as for a product conformity assessment
  - At which level of the organization should an audit as per ISO/SAE 21434 be conducted?
    - Management system audit
    - Process audit
    - Product audit

Answers to the above questions should satisfy the following

- Defined methodology provides optimal results against generally accepted audit criteria
- Minimises costs and efforts for the customer
- Avoid repetitive audits for the supplier

Approach

Overview – Verification Landscape

	3rd Party Audit	2nd Party Audit	Self-Assessment
Audit of Cybersecurity Management System	Certification of the organization's CSMS against standards, rules and regulations	Verification of compliance to standards, rules and regulations beyond existing certification	As part of the mandatory internal control mechanisms of the CSMS and QMS
Process Audit	To the extent industry wide standardized processes exist	As part of supplier management for (contractually) agreed critical processes and interfaces between customer and supplier	As part of the mandatory internal control mechanisms of the CSMS and QMS
Product Conformity Audit	Certification of vehicles and standard components against standardized criteria	As part of the approval procedures during milestones and on final delivery	As part of the mandatory control mechanisms of the CSMS and QMS

Approach

VCS – Positioning in the Verification Landscape

	3rd Party Audit		2nd Party Audit	Self-Assessment
Audit of Cybersecurity Management System	OEMs: UN R-155 Certificate of Compliance	Suppliers: Vehicle Cybersecurity Audit	VDA Automotive Cybersecurity Management System Audit	As part of the mandatory internal control mechanisms of the CSMS and QMS
Process Audit	To the extent industry wide standardized processes exist		Automotive SPICE for Cybersecurity	Automotive SPICE for Cybersecurity
Product Conformity Audit	UN R-155 Vehicle Type Approval / Homologation		As part of the approval procedures during milestones and on final delivery	As part of the mandatory control mechanisms of the CSMS and QMS

Approach

Implementation plan

- Verify the feasibility of a “minimum viable” third party VCS audit scheme (MVA) for the automotive supply chain through piloting audit activities of a standardized third-party V-CSMS audit scheme
- Standardize a third-party Vehicle Cybersecurity Management System audit scheme for the supplier
  - Design the audit scheme in the context of the ISO/SAE 21434 and implement the ISO/PAS 5112
  - Included the generic management system context as defined in Annex SL of the ISO/IEC directives
  - Use ENX’s established audit framework to achieve objective, transparent, comparable and customer-independent results (in contrast to the proprietary certification schemes offered by individual audit providers)

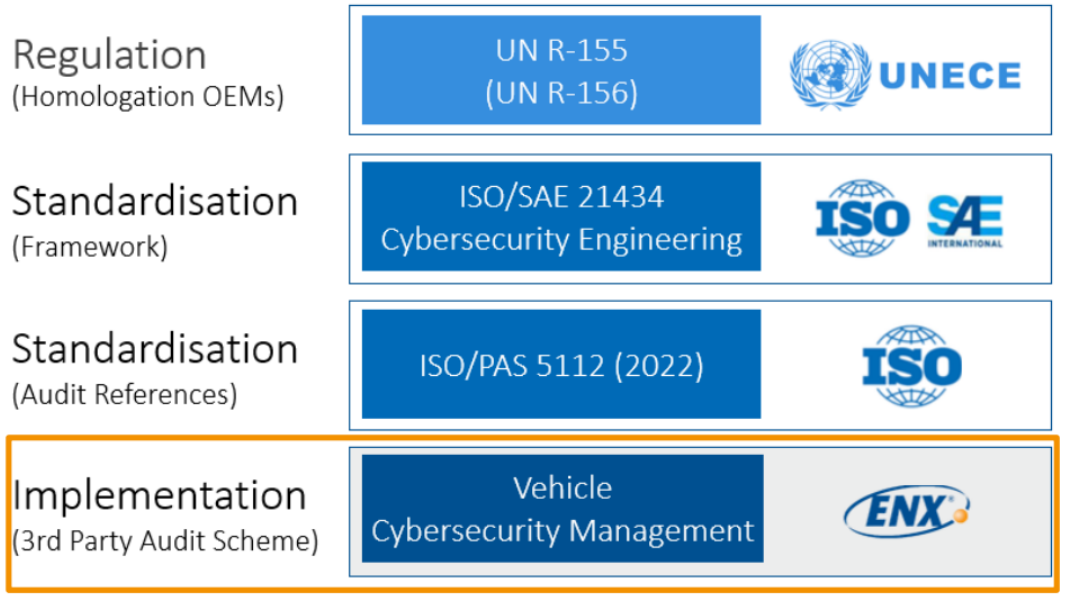


Table of Contents

- Executive Summary
- Motivation
- Objective
- Organization of Project
- Results – Development and piloting of audit scheme
- Recommendations

Organization of Project

Overview – Project Group VCS

Group Type:	Group Name:	Chairperson:	Dpt.-Chairperson:
Project Group	VCS	AUDI	ZF
Number of members (persons):	ENX representant:	Meeting frequency:	Working language:
14	Suhas Konanur Immo Wehrenberg	Monthly (Web Conference)	English

Members:

Audi
Autoliv
AVL
Bertrandt
BMW
Continental
ENX
Mercedes-Benz
Renault
VDA
ZF

- The Project Group comprises of
  - 14 members from
  - 8 organizations
- Project Group Working Duration: September 2021 – September 2023
- Details can be found in the Annex section

Purpose of the group:

- Verify the feasibility of a third party TISAX VCS audit scheme and pilot audit activities for the automotive supply chain
  - Develop a “minimum viable” audit scheme
  - Pilot/evaluation audit activities to verify feasibility
- Work packages to develop and pilot the audit scheme (WP)
  - Definition of VCS audit requirement catalogue
  - Definition of VCS audit scoping mechanisms
  - Definition of VCS audit methodology
  - Definition of VCS auditor qualification requirements
  - Coordination with other (external) VCS activities
  - Piloting of audits
- If feasibility is proven, project group transforms into a working group to work on continuous improvement and maintenance of the audit scheme

Organization of Project

Overview – Resources and Funding by ENX Association

Support by TISAX program lead and management

Dedicated technical project expert – VCS

Funding of pilot audit activities

Total project investment by ENX Association ca. € 500.000

Table of Contents

- Executive Summary
- Motivation
- Objective
- Organization of Project
- Results – Development and piloting of audit scheme
- Recommendations

Results

Work packages to develop and pilot audit scheme

- Defined and developed VCS audit criteria catalogue
- Defined VCS audit scoping mechanisms
- Defined VCS audit methodology
- Developed VCS auditor qualification requirements
- Coordinated with other (external) VCS activities
- Piloted audit activities

Contributions

- PG VCS:
  - Members of the PG VCS accomplished the necessary results, which demonstrate the achievement of the project objective
- ENX support:
  - Provided a first proposal for a solution for VCS audit as basis of discussion and work
  - Provided insight into the solutions and rationale of the deliverables
  - Actively supported work activities

Results

Work packages to develop and pilot audit scheme

- **Defined and developed VCS audit criteria catalogue**
- Defined VCS audit scoping mechanisms
- Defined VCS audit methodology
- Developed VCS auditor qualification requirements
- Coordinated with other (external) VCS activities
- Piloted audit activities

Results:

- PG VCS developed the VCS audit criteria catalogue (VCSA)
- Catalogue has implemented the ISO/PAS 5112 in the context of the ISO/SAE 21434 with relevant inputs from the Annex SL of the ISO/IEC directives
- Mapping of the catalogue with ISO/SAE 21434 and implementation of the ISO/PAS 5112 helps to streamline the CSMS process for supplier organizations, thereby strengthening their cybersecurity posture
- 2-stage piloting of audits with 2 improvement cycles (with 85+ change requests; 10 review sessions) accomplished to validate the catalogue
- Catalogue is available for public release

Details can be found in the annex

Results

Work packages to develop and pilot audit scheme

- Defined and developed VCS audit criteria catalogue
- **Defined VCS audit scoping mechanisms**
- Defined VCS audit methodology
- Developed VCS auditor qualification requirements
- Coordinated with other (external) VCS activities
- Piloted audit activities

Results:

- General scope description for VCS defined
- Scope description consists of following parameters – Audit Objective, Protection Objects and Goals, Audit Level defined for VCS
- 3 new Audit Objectives defined to encompass entire product life cycle of the vehicle
- Protection Objects and Goals defined in VCS context

Details can be found in the annex

Results

Work packages to develop and pilot audit scheme

- Defined and developed VCS audit criteria catalogue
- Defined VCS audit scoping mechanisms
- **Defined VCS audit methodology**
- Developed VCS auditor qualification requirements
- Coordinated with other (external) VCS activities
- Piloted audit activities

Results:

- Standard audit steps and methodology used in TISAX retained
- Audit methodology with highest Audit Level 3 (on-site audits) is applicable for VCS audits
- All piloting audits conducted under Audit Level 3 (on-site)

Details can be found in the annex

Results

Work packages to develop and pilot audit scheme

- Defined and developed VCS audit criteria catalogue
- Defined VCS audit scoping mechanisms
- Defined VCS audit methodology
- **Developed VCS auditor qualification requirements**
- Coordinated with other (external) VCS activities
- Piloted audit activities

Results:

- Auditor qualification levels and corresponding roles used in TISAX retained
- The auditor qualification level for VCS-subject matter expert defined
- VCS subject matter expert: Knowledge areas needed by VCS subject matter expert mapped to corresponding skill levels – Awareness, Practitioner and Expert
- The VCS subject matter expert shall provide an additional role apart from lead auditor and executing auditor in performing VCS audits

Details can be found in the annex

Results

Work packages to develop and pilot audit scheme

- Defined and developed VCS audit criteria catalogue
- Defined VCS audit scoping mechanisms
- Defined VCS audit methodology
- Developed VCS auditor qualification requirements
- **Coordinated with other (external) VCS activities**
- Piloted audit activities

Activities:

- ENX working in the DIN national mirror committee of ISO/TC 22/SC 32/WG 11 on compliance and governance activities pertaining to vehicle cybersecurity
- ENX is on a task force to explore possibilities of expanding the ISO/SAE 21434 into a management system standard

Details can be found in the annex

Results

Work packages to develop and pilot audit scheme

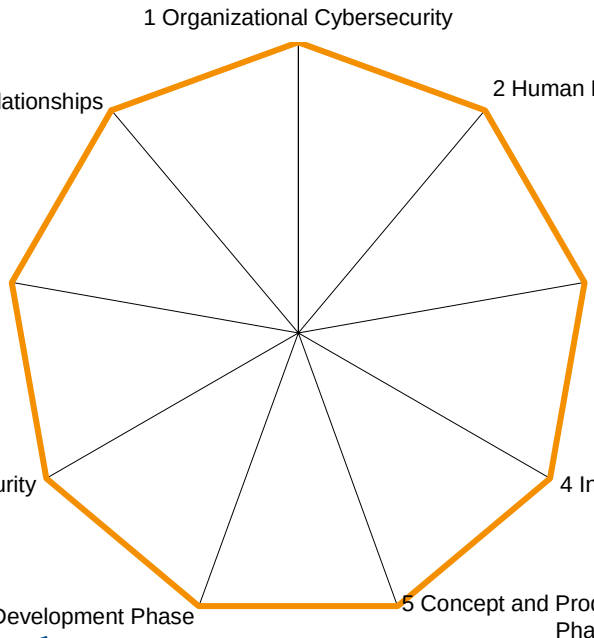
- Defined and developed VCS audit criteria catalogue
- Defined VCS audit scoping mechanisms
- Defined VCS audit methodology
- Developed VCS auditor qualification requirements
- Coordinated with other (external) VCS activities
- **Piloted audit activities**

Results:

- Piloting activities conducted across 6 organizations by 4 audit providers
- The piloting objectives, namely catalogue criteria, performance of the audit teams and auditor qualification requirements were verified
- The audit methodology based on “project sampling” was tested and verified
- 92 findings reported, which represented focal points of CSMS improvement for audit participants

Areas of VCS Audit

Focus of Protection is always the Customer



1 Organizational Cybersecurity

2 Human Resources - Cybersecurity culture

3 Risk Management

4 Internal Assessments

5 Concept and Product Development Phase

6 Post-Development Phase

7 Operations Security

8 Incident Management

9 Supply Chain Relationships

Mapping Audit Objectives to Audit Chapters

Relevant Chapters	Topic	Audit Objectives		
		VCS Development	VCS Production	VCS Operations & Maintenance
1, 2, 3, 4	Organization /Culture/ Risk / Internal Assessment	Compulsory	Compulsory	Compulsory
5	Development	Compulsory	NA	NA
6	Post-Dev./ Production	NA	Compulsory	NA
7, 8	Continual Cybersecurity incl. Incident response	NA	NA	Compulsory
9	Supply Chain	Compulsory	Compulsory	Compulsory

Piloting of audits

Selection of Supplier and Audit Providers

6 pilot audits across relevant supplier profiles

Pilot audit participant selection

- 1 Development service provider
- 3 System/Part manufacturers
- 1 Cybersecurity service provider
- 1 SME

Pilot audit provider selection

- 4 volunteering TISAX Audit Providers
- Identification by ENX in coordination with pilot audit participants
- Selection criteria: Ability to execute VCS audit; auditee preference

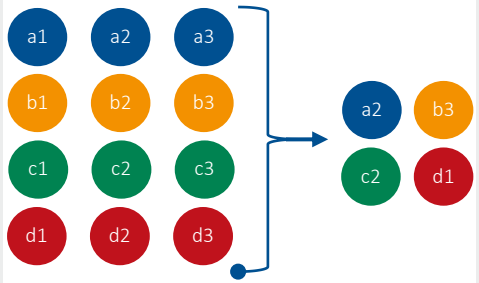
Piloting of audits

Audit focuses on the CSMS and cybersecurity relevant activities (not on locations)

Organizational Check

Establish that the CSMS provides the necessary centralized structures to ensure proper implementation across all projects

- Specified centrally binding cybersecurity policies
- Global responsibility and authority for cybersecurity management
- Global overview over all cybersecurity relevant projects and activities
- Appropriate cybersecurity culture and awareness
- All business units/divisions in scope implement appropriate processes to comply to policies
- Internal audit planning and scheduling including follow-up on results and tracking of implementation of corrective actions



Deep dive of CSMS followed by validation through project sampling

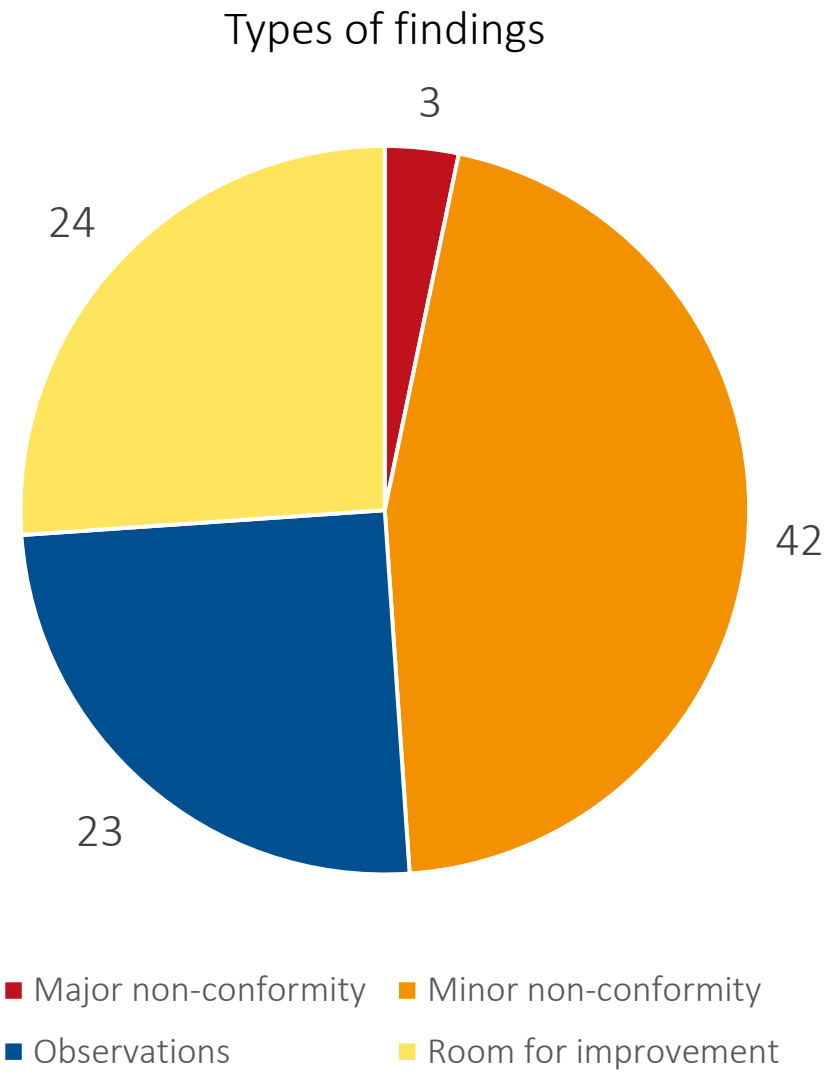
Project Sampling Checks

- Verify the accuracy of the information gathered during the “Organizational Check”
- A minimum number of sample checks is conducted to verify the effective implementation of the CSMS with the smallest total effort
- Sampling parameter is a project selected from a list of projects within the audit scope, where a project involves one or more of development, production and operational maintenance for item(s)
- The project selection occurs after the “Organizational Check”
- If significant deviations identified in implementation vis-à-vis expectations from "Organizational checks", then the sampling project check requirements are not met

Piloting of audits

Results – Datapoints

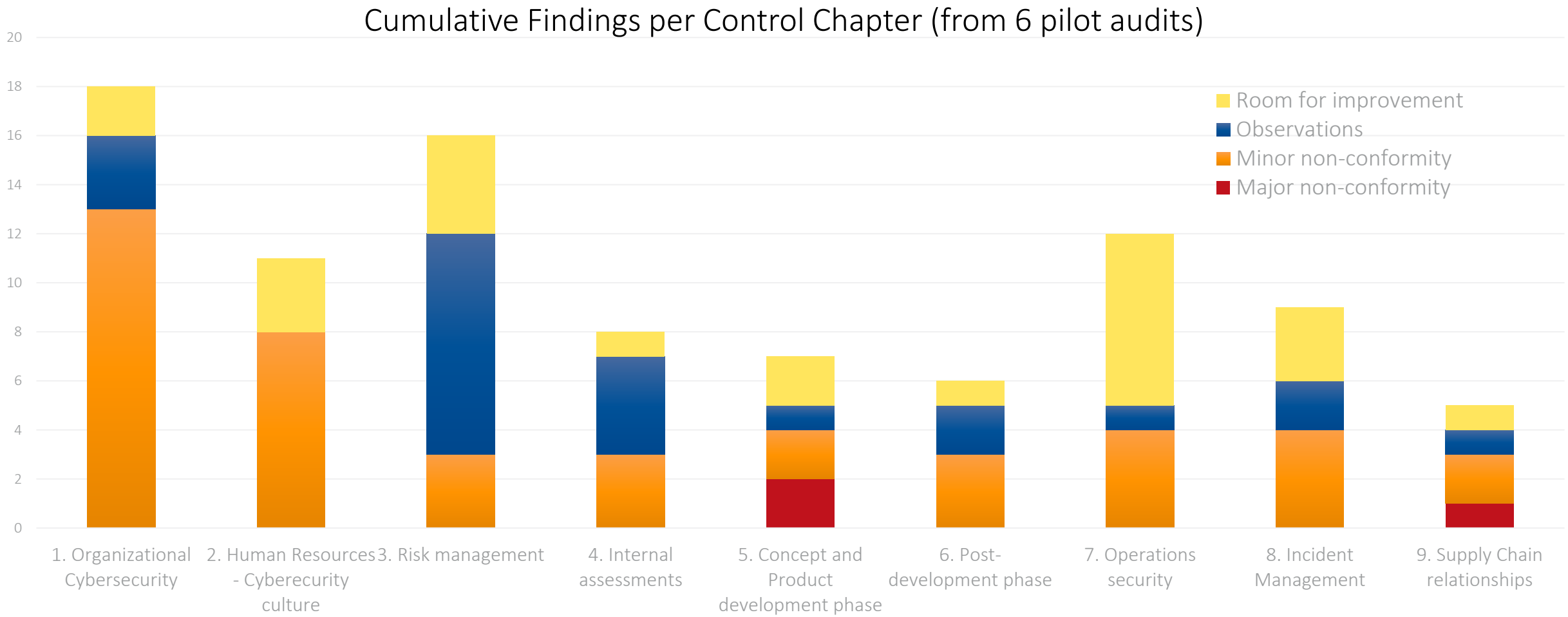
- 6 Audit participants
- 4 Audit Providers
- 50+ Auditor-Days
- 92 Findings



All the numbers and graphs have been generated in a development environment

Piloting of audits

Results – Datapoints



Piloting of audits

Feedback from stakeholders

"Most comprehensive V-CSMS audit we had so far. Outcome is correct and helpful"

-- Expert at large supplier

"Different and very helpful approach adding to existing microchip cybersecurity requirements from other Industries"

-- Lead Auditor

"Most promising approach to establish a broadly accepted V-CSMS audit standard and better than our own individual approach

-- Product line director of audit provider

"Very comprehensive audit that can certainly be used as very solid evidence in R-155 CoC audits"

-- R-155 and V-CSMS expert

"Catalogue is much easier, better structured and easier to understand than the underlying standards"

-- Lead Auditor

Piloting of audits

Conclusions concerning the objectives of piloting

Implementation of audit scheme

- Verified implementation of requirements of ISO/SAE 21434 and ISO/PAS 5112 as well as Annex SL of the ISO/IEC directive

Effectiveness of audit scheme

- Evaluated the scope of the CSMS and its effectiveness across applicable phases of product lifecycle
- Verified effectiveness through in-depth audit of sampled project(s)
- Ensured ease of audit preparation and “lessons learned” dividends for suppliers especially for SMEs

Maturity of audit scheme

- Confirmed Audit Objectives, and Audit Criteria Catalogue incl. controls and requirements by covering relevant supplier profiles (engineering and software development service providers; automotive system suppliers; leading IT-security provider)
- Verified CSMS interdependencies with information security, functional safety and quality management

Piloting of audits

Conclusions concerning the objectives of piloting

Performance of audit providers and audit teams

- Performed audit activities from kick-off follow-up in a transparent, standardized and reliable way
- Verified appropriateness of existing audit framework to ensure consistent quality, depth and scope of audit activities

Auditor qualification requirements

- Evaluated the proficiency in knowledge areas mentioned in the VCS role for cybersecurity expert sufficient to competently discharge audit responsibilities
- Confirmed the necessity for at least a lead auditor role and automotive cybersecurity expert role to execute a holistic audit

Table of Contents

- Executive Summary
- Motivation
- Objective
- Organization of Project
- Results - Development and piloting of audit scheme
- Recommendations

Recommendation

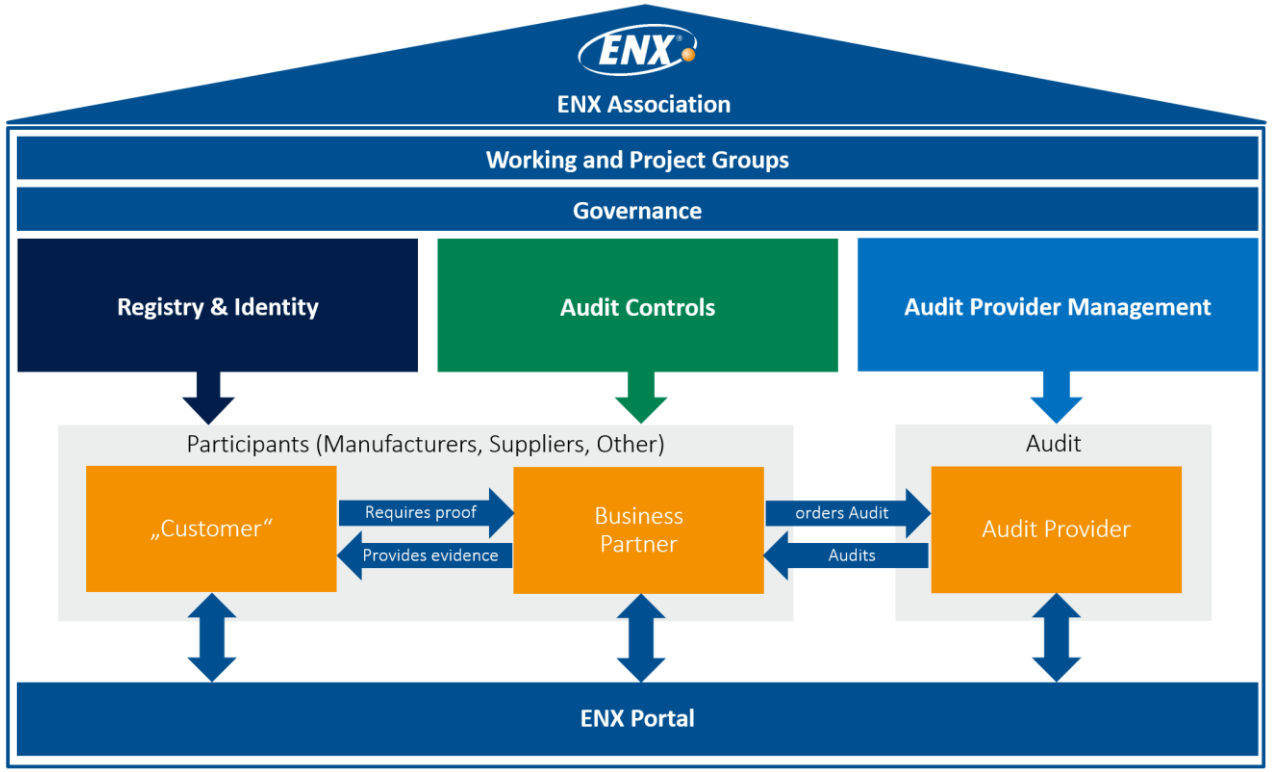
Make VCS audit publicly available

- PG VCS acknowledges that the audits conducted during piloting activities provide an accurate and representative result of the CSMS capability of the audited organizations
- PG VCS recommends that the developed, piloted and revised VCS audit be made available to interested parties
- PG VCS recommends to recognise the results gained during piloting

Recommendations

Leverage ENX framework for Vehicle Cybersecurity

- Extend existing structures to involve automotive vehicle cybersecurity stakeholders for an international industry wide acceptance
- Transform PG VCS into a working group to continuously improve and maintain VCS scheme with representatives of the industry
- Expand on existing ENX contractual framework to encompass VCS audits
- Integrate VCS participants into ENX Portal with necessary user interface and processes
- Utilize ENX Portal to share information on audit objectives and labels achieved
- Develop and publish documentation



Recommendations

Standardization of VCS scheme

- Selection of audit participant whose scope corresponds to only one Audit Objective
- Adaptable „no one-size-fits-all“ approach for TARA (Threat Analysis and Risk Assessment) needs to be formulated
  - TARA methodology varies from component level (especially out-of-context components) to system level – audit to be conducted appropriately
  - TARA methodology for organizations in other industrial domains that collaborate with the automotive industry and whose products subscribe to cybersecurity standards other than ISO/SAE 21434 (like Common Criteria, GSMA, C5 etc.)
- Participate in ISO/SAE PAS 8475 CAL-TAF and ISO/SAE PWI 8477 V&V and integrate these standards to the VCS audit criteria catalogue.

Recommendations

Auditing different supplier profiles

- ISO/SAE 21434 is intended for “in-context” and “out-of-context” development
  - Off-the-shelf products, which are industry and domain agnostic, are considered out of scope
- Risk management „adapted“ based on intended use
  a) Suppliers developed „in-context“ customer project specific solutions OR
  b) Suppliers developed solutions as a component „out-of-context“
    - Tailoring is applicable (Assumptions determine TARA, cybersecurity concept, cybersecurity case)
    - Verify if the assumptions on intended use was created and communicated to customer (cybersecurity concept and case)
- Supply chain relationship
  - Supplier engages with customer using a full-fledged DIA (Development Interface Agreement) for distributed development
  - For out-of-context components, instead of DIA, verify if supplier provides customer information regarding component integration and incident reporting

Recommendations

VCS audit – baseline for other audits

- VCS audit relies on completed ISMS audits (e.g., TISAX)
  - No redundant ISMS questions in VCS catalogue
- Leverage synergy CSMS – ISMS in the following areas
  - Management level policy formulation
  - Tool management
  - Software updates
  - Cybersecurity in Production – Key management
  - Supplier management
- Customer-specific process audits (e.g., ASPICE) can build on the foundation provided by VCS

United Nations ECE/TRANS/WP.29/2020/79 REVISED

Economic and Social Council

Distr.: General
23 June 2020

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

"7.2.2.5. The vehicle manufacturer shall be required to demonstrate 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."

The following could be used to evidence the processes used:

(f) Contractual agreements in place or evidence of such agreements;

(g) Evidenced arguments for how their processes will ensure suppliers / service providers will be considered in the risk assessment process;

(h) Procedures/Methods of sharing information on risk between suppliers and manufacturers;

(i) Existing solutions / contracts like ISMS (Information Security Management System) regulation can be used for evidence. This may be evidenced by certificates based on ISO/IEC 27001 or TISAX (Trusted Information Security Assessment eXchange).

Recommendations

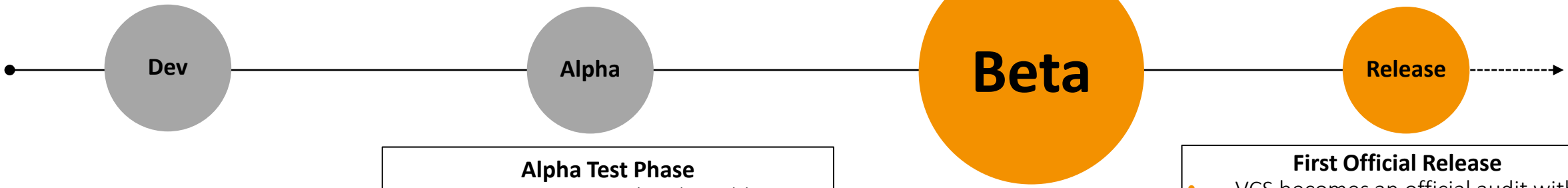
VCS - Way ahead - BETA phase

Development Phase

- Definition and coordination of an Initial draft of VCSA
- Definition and coordination of initial draft of VCS Audit Scheme details such as scoping, audit execution and auditor qualification
- Make everything ready for alpha-test

Beta Test Phase

- Public real-world testing
- Information is released as draft (available to all stakeholders)
- No known unfinished aspects or significant shortcomings (but documentation and experience may be still lacking)



Alpha Test Phase

- Private experimental real-world testing
- Information is not released; development snapshots are shared only with participants selected for testing
- Some aspects are not yet defined and some uncertainty for audit outcome still exists

First Official Release

- VCS becomes an official audit within ENX framework (“Official Release”)
- Information is released as official version (available to all stakeholders)
- Fully defined and tested audit and documentation, fixed outcome, changes within regular continuous improvement cycles

Initial Contact

+49 69 9866927-71
vcs@enx.com

ENX Association

an Association according to the French Law
of 1901,registered under No. W923004198
at Boulogne-Billancourt, France.

Addresses

20 Rue Danjou, 92100 Boulogne-Billancourt, France
Bockenheimer Landstraße 97-99, 60325 Frankfurt, Germany

Intellectual Property

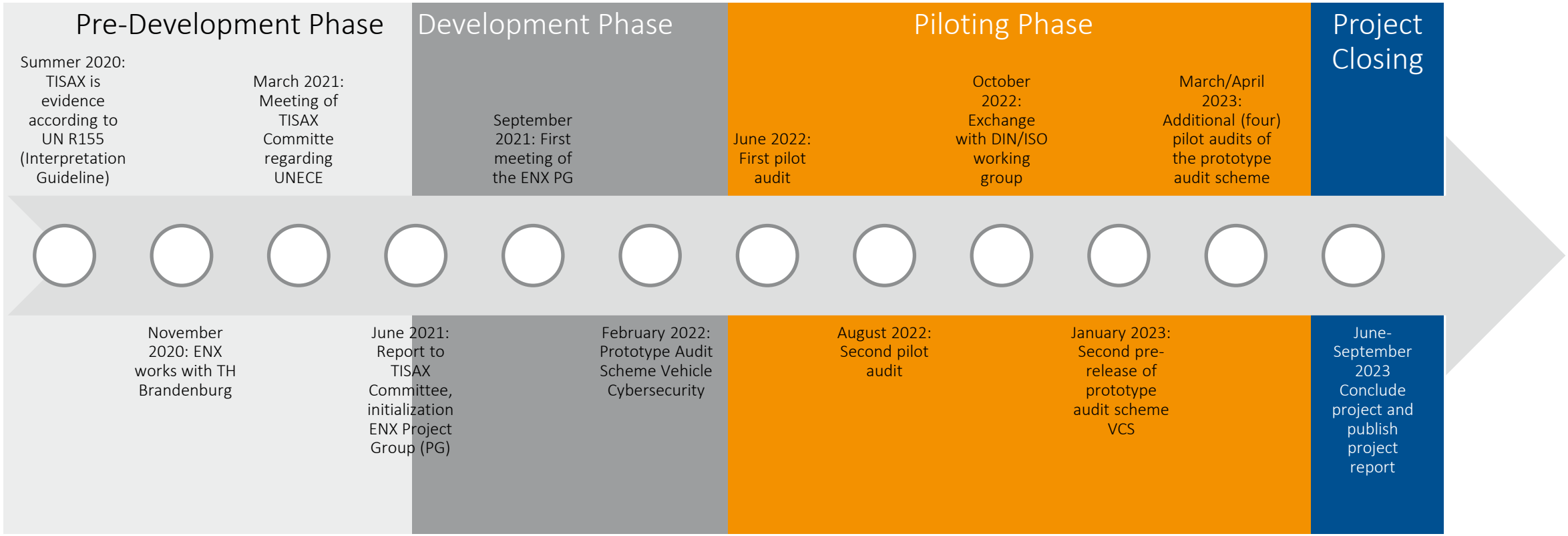
www.enx.com

X

Annex

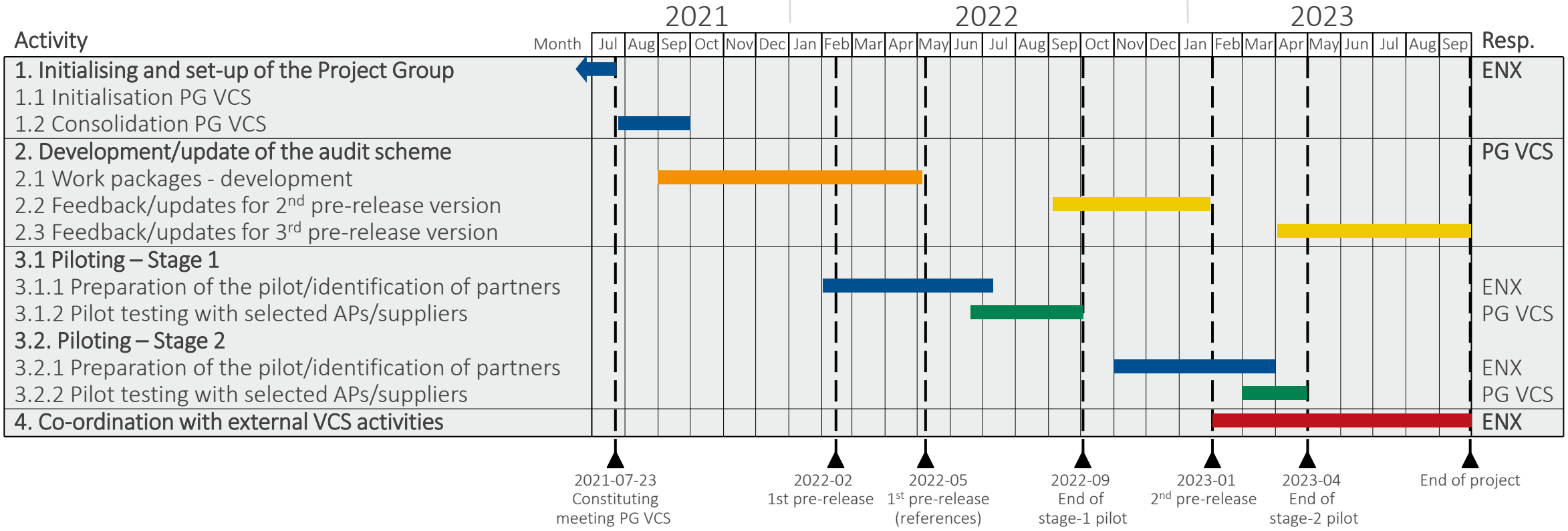
Organization of Project

VCS Audit – Timeline



Organization of Project

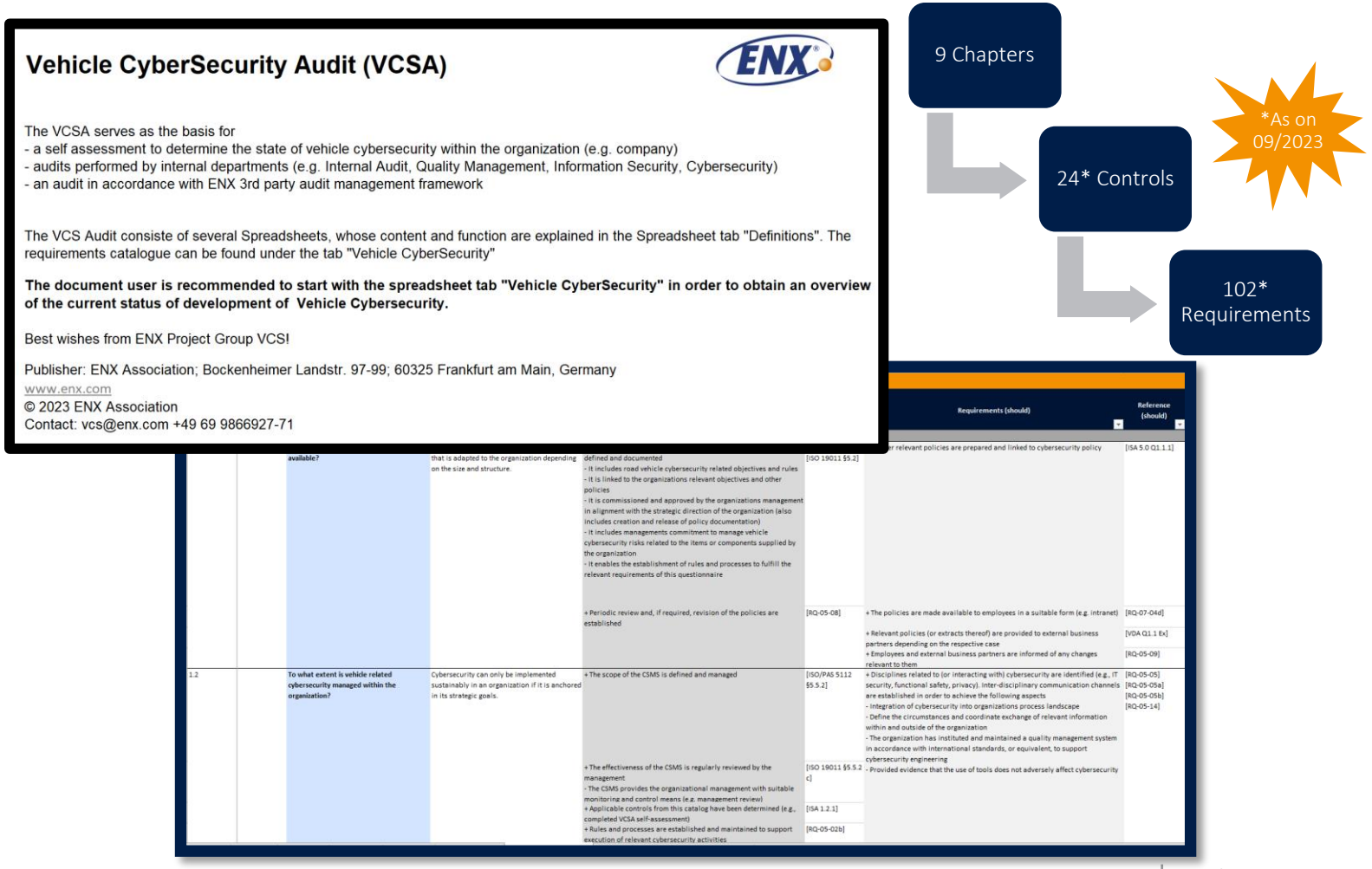
VCS – Detailed implementation timetable



WP – Audit Requirement Catalogue

Overview

- The catalogue consists of control questions and requirements classified into various chapters
- The catalogue has adapted the format and structure to the specific needs of CSMS related to vehicle cybersecurity suppliers
- The requirements of the catalogue are traceable to the ISO/SAE 21434
- A proven format that provides familiarity and ease of use for stakeholders



WP – Audit Requirement Catalogue

Development of Catalogue

Approach

- Explored approaches and requirements to vehicle cybersecurity and the differences to organizational information security
  - Different Protection Objects and Protection Goals vis-à-vis organizational information security
  - Hence new control questions and requirements need to be formulated
- Explored prerequisites for VCS audit: Audit participant to have a functioning and valid ISMS

Applicable Protection goals and Protection objects for VCS

WP – Audit Requirement Catalogue

Development of Catalogue

Implementation

- The UN Regulation No. 155 mandates requirements concerning the approval of vehicles with regards to CSMS
- The ISO/SAE 21434 is an engineering standard to assist implementation of CSMS to organizations along the supply chain
- ISO/PAS 5112 provides guidelines on conducting management system audits along with a set of audit criteria based on the objectives of the ISO/SAE 21434
- VCS catalogue implements the ISO/PAS 5112 in the context of the ISO/SAE 21434 with relevant inputs from the Annex SL of the ISO/IEC directives - generic management system structure and provides a standard set of audit criteria

WP – Audit Requirement Catalogue

Development of Catalogue

Implementation

Mapped the catalogue chapters/topics, control questions and requirements to VCS Audit Objectives

Mapping Control Catalogue with Audit Objectives

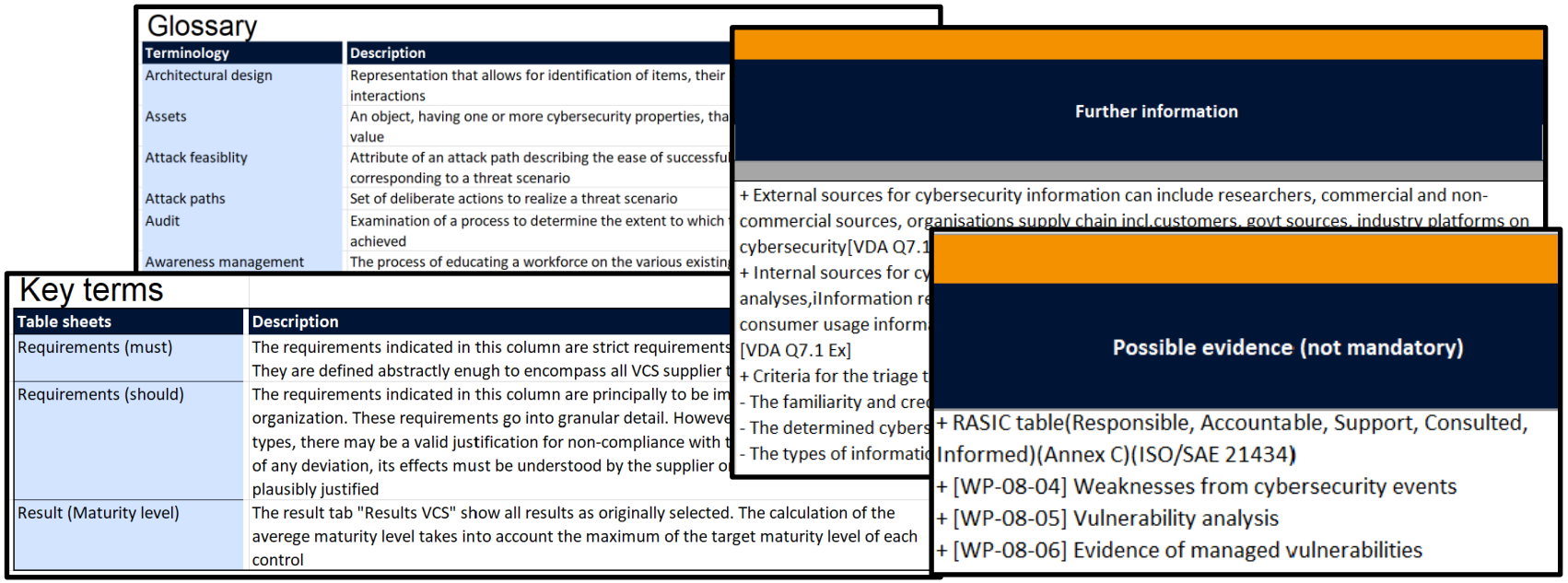
Relevant Control questions	Topic	Assessment Objectives		
		VCS Development	VCS Production	VCS Operations & Maintenance
1.1-4.1	Organization /Culture/ Risk / Internal Assessment	Compulsory	Compulsory	Compulsory
5.1-5.3	Development	Compulsory	N/A	N/A
6.1-6.2	Post Dev.	N/A	Compulsory	NA
7.1-8.3	Continual Cybersecurity incl. Incident response	N/A	N/A	Compulsory
9.1	Supply Chain	Compulsory	Compulsory	Compulsory

WP – Audit Requirement Catalogue

Development of Catalogue

Implementation

- “Further information” and “Evidences” in the requirements catalogue provide supporting information for audit stakeholders
- Vehicle Cybersecurity specific “Glossary” and definition of “Key Terms” was created



Glossary

Terminology	Description
Architectural design	Representation that allows for identification of items, their interactions
Assets	An object, having one or more cybersecurity properties, tha value
Attack feasiblity	Attribute of an attack path describing the ease of successfu corresponding to a threat scenario
Attack paths	Set of deliberate actions to realize a threat scenario
Audit	Examination of a process to determine the extent to which achieved
Awareness management	The process of educating a workforce on the various existin

Key terms

Table sheets	Description
Requirements (must)	The requirements indicated in this column are strict requirements They are defined abstractly enugh to encompass all VCS supplier t
Requirements (should)	The requirements indicated in this column are principally to be im organization. These requirements go into granular detail. Howeve types, there may be a valid justification for non-compliance with t of any deviation, its effects must be understood by the supplier o plausibly justified
Result (Maturity level)	The result tab "Results VCS" show all results as originally selected. The calculation of the averege maturity level takes into account the maximum of the target maturity level of each control

Further information

+ External sources for cybersecurity information can include researchers, commercial and non-commercial sources, organisations supply chain incl.customers, govt sources, industry platforms on cybersecurity[VDA Q7.1
+ Internal sources for cy analyses,iInformation re consumer usage informa [VDA Q7.1 Ex]
+ Criteria for the triage t
- The familiarity and cre
- The determined cybers
- The types of informatic

Possible evidence (not mandatory)

+ RASIC table(Responsible, Accountable, Support, Consulted, Informed)(Annex C)(ISO/SAE 21434)
+ [WP-08-04] Weaknesses from cybersecurity events
+ [WP-08-05] Vulnerability analysis
+ [WP-08-06] Evidence of managed vulnerabilities

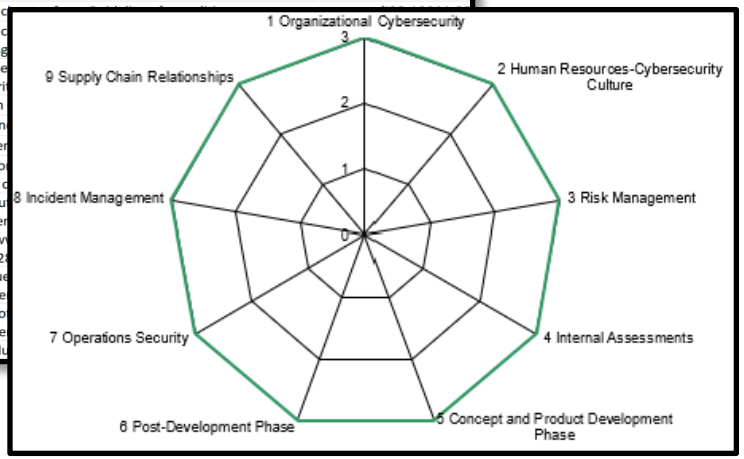
WP – Audit Requirement Catalogue

First pre-release “ALPHA” update

- Pre-release for pilot “ALPHA” audits (from 19.01.2023 onwards)
  - Applicable maturity levels reduced from 5 to 3
  - Maturity labels do not appear either in the report or in the labels. They are meant for internal consumption at the audit participant only
  - Chapters rearranged in the Control Catalogue
    - Chapters renumbered and new chapter “Human resources – Cybersecurity culture” added
  - “References” sheet created describing references to the requirements of the control catalogue
- Activities towards real-world public “BETA” release
  - Draft version available - Option to sort chapters and control questions in line with ISO/PAS 5112
  - After ALPHA audits, 85+ change requests from stakeholders discussed in 10 working sessions
  - Feedbacks from stakeholders involved in pilot audits have been incorporated for release into the control catalogue

Vehicle Cyber Security Assessment
List of references

Reference	Description
[ISA 5.0 Qx.x]	Control questions from VDA Information Security Assessment
[ISO 19011 §x.x]	Reference c
[ISO/PAS 5112 §x.x]	Reference c engineering
[ISO/PAS 5112 Qx.x]	Control que cybersecuri
[PM-xx-yy]	Permission
[RC-xx-yy]	Recommen
[RQ-xx-yy]	Requiremer
[UN R-155, Annex 5]	Proposal fo regards to c
[VDA DIA]	Position Au with referer https://ww 74b6ceb72
[VDA Qx.x]	Control Que Manageme
[VDA Qx.x Ex]	Examples o Manageme
[WP-xx-yy]	Work produ



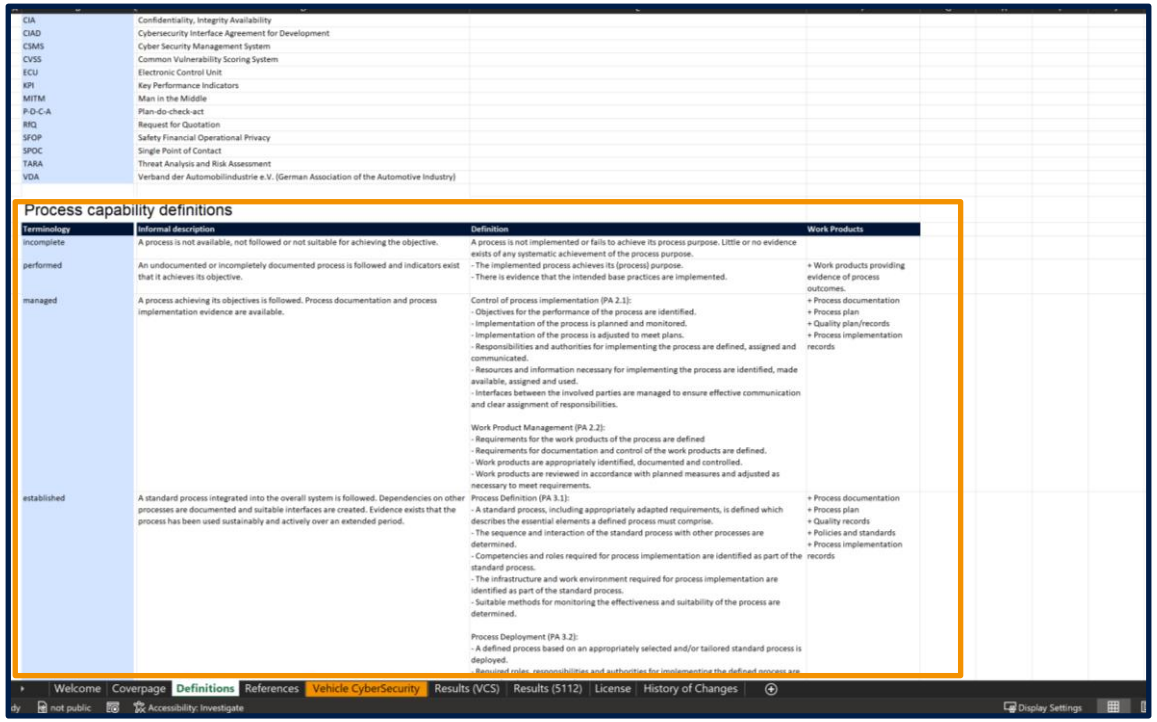
Change-log VCS

1	2b	2c	3	4	5	6a	6b	6c	
Serial No.	Control Question	Column (Control Question, must, should etc)	Responsible	Previous wording	Change suggestion / new wording	Type of change (editorial, significant, ...) (opt.)	Reason for change (opt).	Comment by review members(opt.)	Date of change entry (Responsible person)
19	9,1	Control Question	Suhas Konanur	To what extent are contractual obligations between the auditee organization and its	To what extent are **dependencies** between the auditee organization and its suppliers managed?	significant	Contractual obligations are unique 1-1 obligations between auditee and a particular supplier. Not all auditees are	PG VCS has agreed to implement the change in terminology	26.03.2023

WP – Audit Requirement Catalogue

Release “BETA” update

- No maturity model as per stakeholder feedback
- Process capability definition added to the sheet “Definitions”



CIA	Confidentiality, Integrity Availability
CIAD	Cybersecurity Interface Agreement for Development
CSMS	Cyber Security Management System
CVSS	Common Vulnerability Scoring System
ECU	Electronic Control Unit
KPI	Key Performance Indicators
MITM	Man in the Middle
P-D-C-A	Plan-do-check-act
RfQ	Request for Quotation
SFOP	Safety Financial Operational Privacy
SPOC	Single Point of Contact
TARA	Threat Analysis and Risk Assessment
VDA	Verband der Automobilindustrie e.V. (German Association of the Automotive Industry)

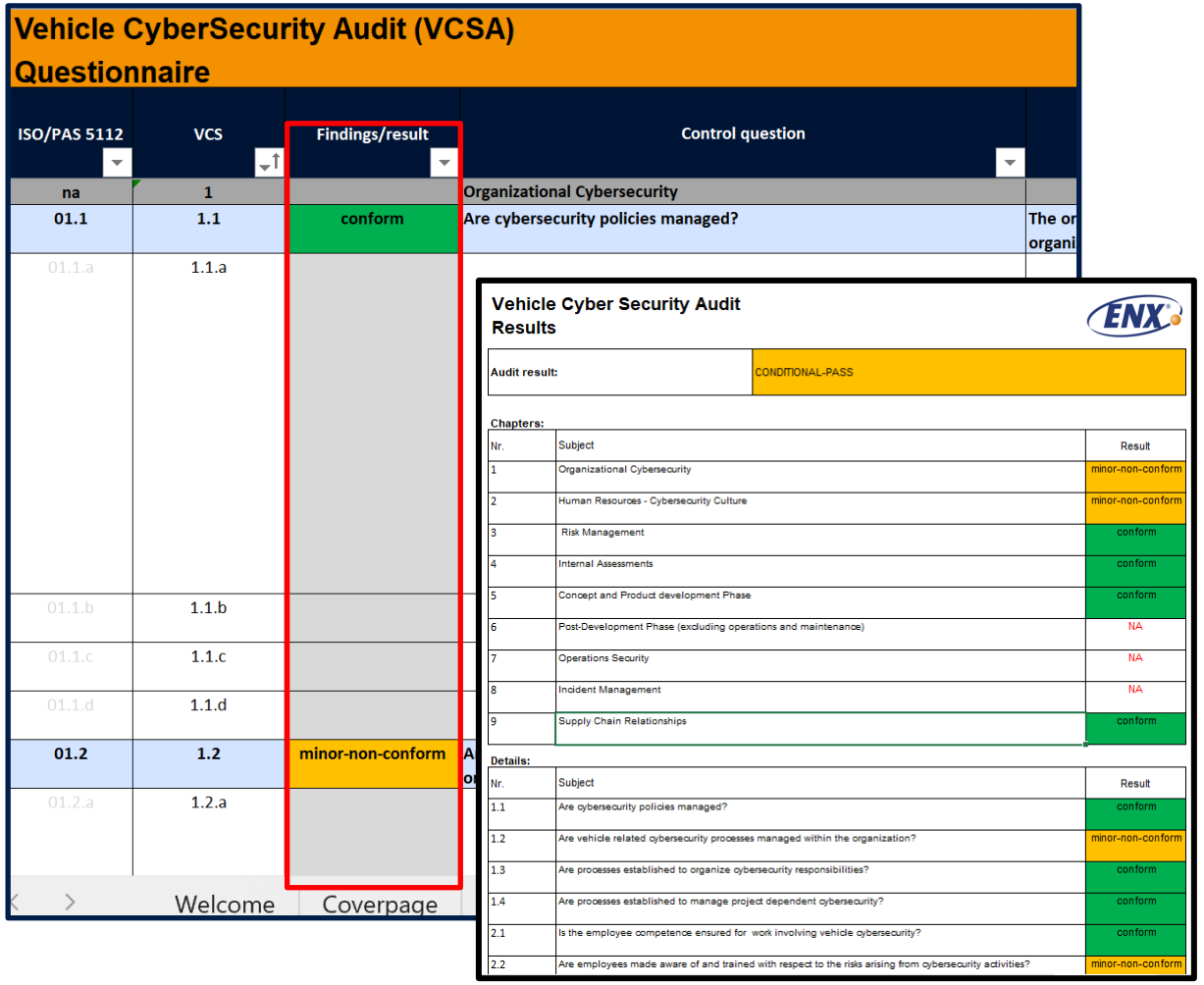
Process capability definitions

Terminology	Informal description	Definition	Work Products
incomplete	A process is not available, not followed or not suitable for achieving the objective.	A process is not implemented or fails to achieve its process purpose. Little or no evidence exists of any systematic achievement of the process purpose.	
performed	An undocumented or incompletely documented process is followed and indicators exist that it achieves its objective.	- The implemented process achieves its (process) purpose. - There is evidence that the intended base practices are implemented.	+ Work products providing evidence of process outcomes.
managed	A process achieving its objectives is followed. Process documentation and process implementation evidence are available.	Control of process implementation (PA 2.1): - Objectives for the performance of the process are identified. - Implementation of the process is planned and monitored. - Implementation of the process is adjusted to meet plans. - Responsibilities and authorities for implementing the process are defined, assigned and communicated. - Resources and information necessary for implementing the process are identified, made available, assigned and used. - Interfaces between the involved parties are managed to ensure effective communication and clear assignment of responsibilities. Work Product Management (PA 2.2): - Requirements for the work products of the process are defined - Requirements for documentation and control of the work products are defined. - Work products are appropriately identified, documented and controlled. - Work products are reviewed in accordance with planned measures and adjusted as necessary to meet requirements.	+ Process documentation + Process plan + Quality plan/records + Process implementation records
established	A standard process integrated into the overall system is followed. Dependencies on other processes are documented and suitable interfaces are created. Evidence exists that the process has been used sustainably and actively over an extended period.	Process Definition (PA 3.1): - A standard process, including appropriately adapted requirements, is defined which describes the essential elements a defined process must comprise. - The sequence and interaction of the standard process with other processes are determined. - Competencies and roles required for process implementation are identified as part of the standard process. - The infrastructure and work environment required for process implementation are identified as part of the standard process. - Suitable methods for monitoring the effectiveness and suitability of the process are determined. Process Deployment (PA 3.2): - A defined process based on an appropriately selected and/or tailored standard process is deployed.	+ Process documentation + Process plan + Quality records + Policies and standards + Process implementation records

WP – Audit Requirement Catalogue

Release “BETA” update

- The result pages show the conformity of each control question
- A drop-down menu is provided to select the relevant “finding” for every control question
- The results are portrayed for every control question and for every chapter
- The overall audit result is Pass / Conditional-Pass / Fail) as recommended by ISO/PAS 5112
- The questions in the catalogue can be sorted as per “ISO/PAS 5112” or “VCS”
  - The sorting for ISO/PAS 5112 occurs as per the chapters and questions mentioned in the 5112 questionnaire



Vehicle CyberSecurity Audit (VCSA) Questionnaire

ISO/PAS 5112	VCS	Findings/result	Control question	
na	1		Organizational Cybersecurity	
01.1	1.1	conform	Are cybersecurity policies managed?	The or organi
01.1.a	1.1.a			
01.1.b	1.1.b			
01.1.c	1.1.c			
01.1.d	1.1.d			
01.2	1.2	minor-non-conform		
01.2.a	1.2.a			

Welcome | Coverpage

Vehicle Cyber Security Audit Results

Audit result:	CONDITIONAL-PASS

Chapters:

Nr.	Subject	Result
1	Organizational Cybersecurity	minor-non-conform
2	Human Resources - Cybersecurity Culture	minor-non-conform
3	Risk Management	conform
4	Internal Assessments	conform
5	Concept and Product development Phase	conform
6	Post-Development Phase (excluding operations and maintenance)	NA
7	Operations Security	NA
8	Incident Management	NA
9	Supply Chain Relationships	conform

Details:

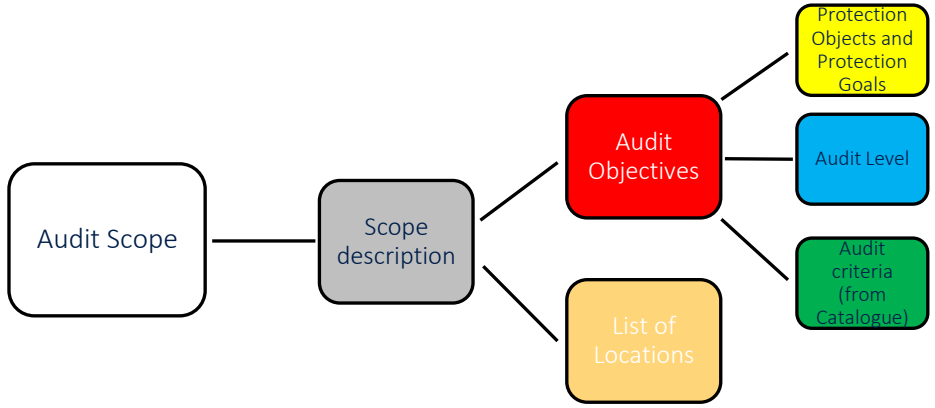
Nr.	Subject	Result
1.1	Are cybersecurity policies managed?	conform
1.2	Are vehicle related cybersecurity processes managed within the organization?	minor-non-conform
1.3	Are processes established to organize cybersecurity responsibilities?	conform
1.4	Are processes established to manage project dependent cybersecurity?	conform
2.1	Is the employee competence ensured for work involving vehicle cybersecurity?	conform
2.2	Are employees made aware of and trained with respect to the risks arising from cybersecurity activities?	minor-non-conform

WP - VCS Audit Scoping Mechanisms

- The Standard Scope facilitates the modular scoping approach using VCS Audit Objectives and the list of locations
- The scope covers the security aspects of the protection objects and protection goals for the selected audit objectives
- Labels awarded for the selected audit objectives at the listed locations upon successful completion of the audit
- Definition of Standard Scope Description (v2.0.1)

  "The Scope defines the scope of the audit. The audit includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the selected audit objectives at the listed locations

  The audit is conducted at least in the highest Audit Level listed in any of the listed Audit Objectives. All audit criteria listed in the selected audit objectives are subject to the audit "



TISAX VCS - Definition of audit objectives and their protection goals

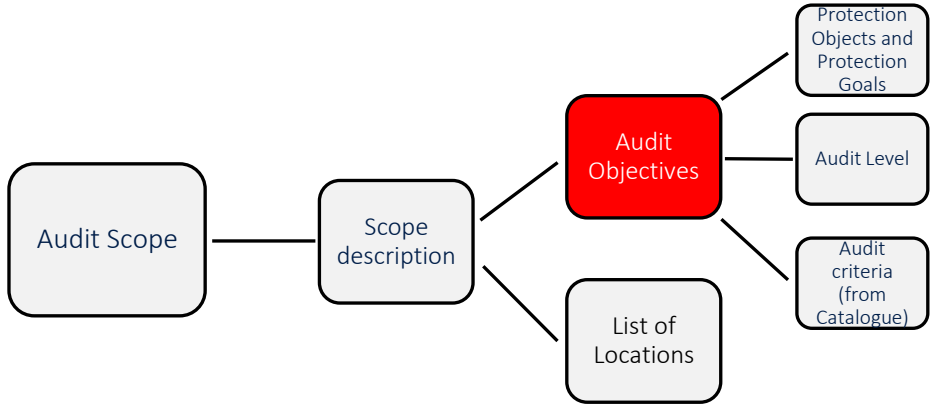
WP - VCS Audit Scoping Mechanisms

List of Audit Objectives

- Defined VCS Audit Objectives to accommodate different supplier profiles
- The number of applicable Audit Objectives for the supplier is determined by the relevant stages of the product lifecycle the supplier is involved in

Audit Objectives	Description
VCS Development	Concept phase, product development phase, integration, verification and validation
VCS Production	Production phase incl. injection of (SecOC) keys, secure booting of microcontrollers, flashing of TLS certificates etc
VCS Operations & Maintenance	Monitoring information; event and weakness analysis; vulnerability management; incident response; cybersecurity relevant updates and end-of-life activities (reliable deletion of keys and certificates during scrapping)

The listed audit objectives cover the entire vehicle product life cycle and CSMS scope of the audited organizations



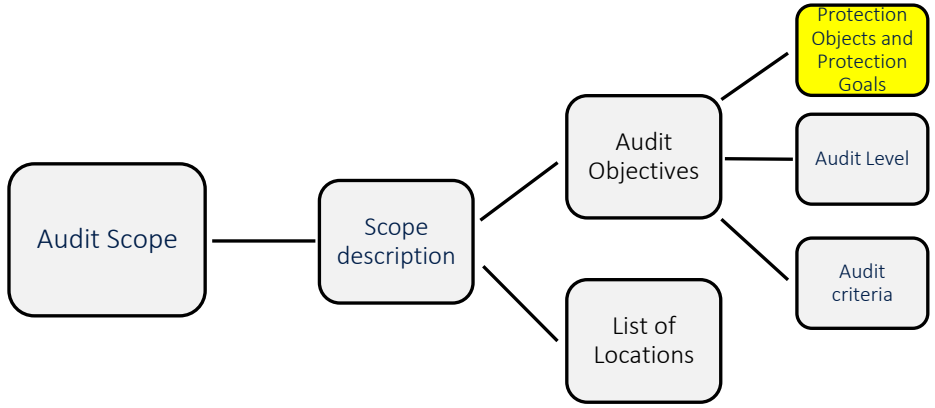
VCS - Definition of audit objectives and their protection goals

WP - VCS Audit Scoping Mechanisms

Description of Protection Objects and Goals

- Protection Objects:
  - Assets in items and components with cybersecurity properties
  - Cybersecurity properties include confidentiality, integrity and availability. Further properties include authentication, authorization and non-repudiation

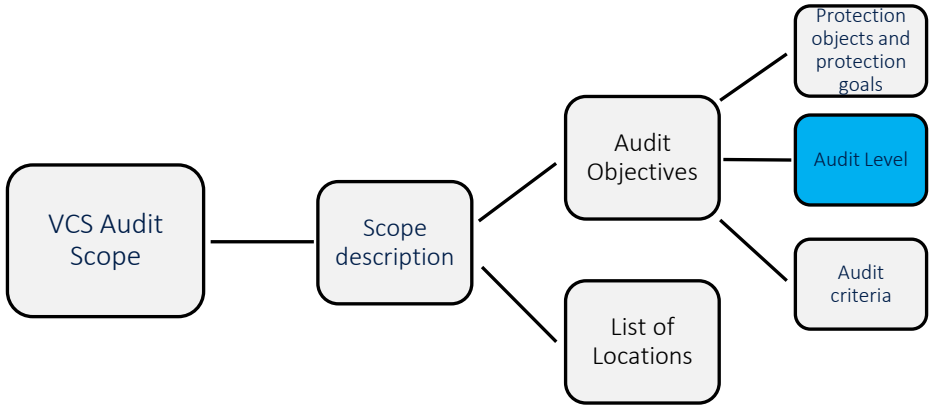
- Protection Goals:
  - Protection of *Audit Objects* against cyber threat scenarios relevant for road vehicles

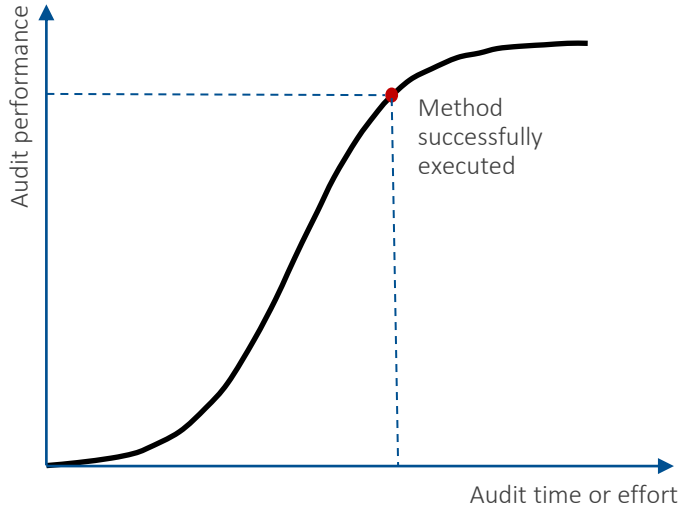


VCS - Definition of Audit Objectives and their Protection Goals

WP – Audit Methodology

- Brief overview of the audit methodology for VCS
  - Kick-off meeting – audit dates and required documents are determined
  - Self-assessment by audit participant
  - Initial audit – as per defined Audit Levels (ALs)
    - Scope description
    - Audit Objectives
    - List of locations
  - Corrective Action Plan
  - Follow-up Audit
- VCS feasibility audits to be conducted at the *highest Audit Level 3*
  - Full audit including evaluation of evidences, on-site inspection and expert interviews
  - Audit Level 3 to be evaluated for the individual audit objectives
  - A successful audit optimises the audit time/effort taken to achieve the necessary audit performance

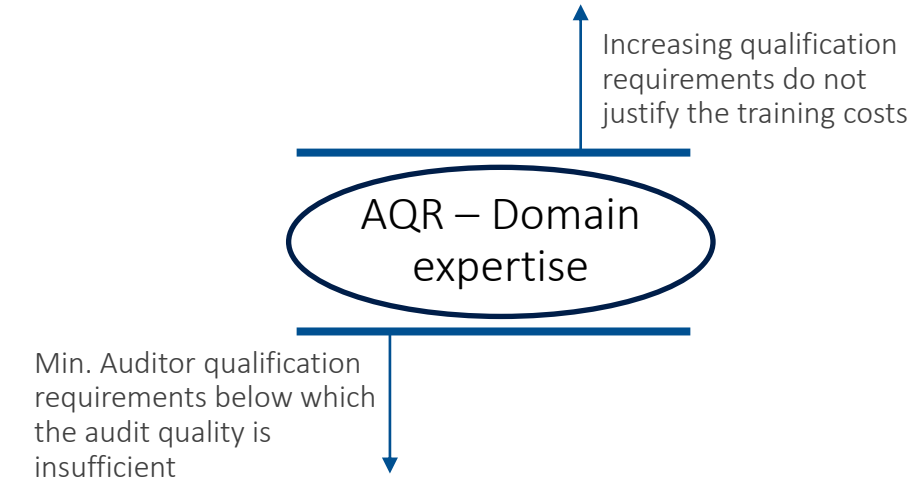




WP – Auditor Qualification Requirements (AQR)

Audit Team Roles for VCS

- An auditing process comprises of many underlying sub-roles
- An audit team can have 1-3 auditors, who can adopt one or multiple sub-roles (makes business sense!)
- Sub-roles are primarily based on
  - Knowledge of management systems
  - Knowledge of auditing methods
  - Knowledge of ENX VCS Audit
  - Domain expertise – automotive cybersecurity
    - Achieve a balance between min. auditor qualification requirements and the costs of auditor training



WP – Auditor Qualification Requirements

Audit Team Role – VCS Expert

Knowledge areas	Typical knowledge and skills in:	Practitioner	Expert	Awareness
Organizational cybersecurity AND Human Resources - Cybersecurity culture	Policies and procedures	x		
	Roles, responsibilities and organizational structures or cybersecurity, competence and awareness management	x		
	Cybersecurity planning of activities (TARA, Work products)	x		
Risk management	Standards, processes, techniques, methods and practices used for cybersecurity, including management measures as well as an appropriate level of technical expertise	x		
	TARA methods including risk assessment based on asset identification,damage scenarios, threat scenarios and attack paths, attack tree analysis		x	
Internal assessment	Internal audits (product development), assessments such as ASPICE		x	
Concept and product development phase	E/E Requirements Engineering for HW, SW and Systems		x	
	Automotive technology (in-vehicle, backend, safety related architecture)		x	
	Testing procedures for cybersecurity (integration tests, functional tests, penetration testing or fuzz testing)		x	
Post-development phase	Vehicle lifecycle management	x		
	Cybersecurity in the production		x	
Operations security	Threat intelligence, vulnerability management and cybersecurity activities for post-production (Updates, end of support and decommissioning activities)		x	
Incident management	Processes and involved stakeholders for cybersecurity incident response		x	
Supply chain relationship	Automotive supply chain and distributed cybersecurity activities w.r.t CSMS		x	
Others	Requirements in the TISAX VCS Catalogue	x		
	Information Security, Functional Safety and their interdependency with cybersecurity (e.g. safety, financial, operational, data protection and privacy)			x

		Management Systems	Auditing	TISAX	Domain expertise
E-04 – Vehicle Cybersecurity Expert	General Requirement	• Knowledge of rules and regulations related to CSMS • Knowledge of UN R-155 and security aspects of UN R-156	• Internal auditing of cybersecurity (nice to have)	Knowledge of requirements in the TISAX VCS Catalogue	
	Evidence for Appointment	n/a	n/a	n/a	Evidence for previous engagements at automotive companies: a. 1- 2 years FTE qualification in CSMS auditing, or b. Record of completion of training courses relevant to CSMS auditing, or c. Proof of competence in automotive cybersecurity through professional development records, or d. Explicit confirmation of sufficient experience and qualification by ENX

WP - Coordinate with Other (External) VCS Activities

Co-Operation with DIN TC22/SC32/WG 11

- Task Force - expanding ISO/SAE 21434 as a management system compliant standard
  - Mapping the Annex SL from ISO/IEC directives to ISO/SAE 21434 (gap-analysis)
  - Justification study (planned)
- VCS Change proposals for ISO/PAS 5112 on 2023-05-9/10
  - Constructive discussion with DIN WG
  - Flexibility to implement the proposals in an audit scheme (such as VCS scheme) based on the ISO/PAS 5112
  - Next version ISO/SAE 21434 to incorporate management system proposals
    - ISO/PAS 5112 (if still valid) to refer to the next version of ISO/SAE 21434