PUBLICLY
AVAILABLE
SPECIFICATION

ISO/PAS 5112

First edition
2022-03

Road vehicles — Guidelines for auditing cybersecurity engineering

Véhicules routiers — Lignes directrices pour l'audit de l'ingénierie de la cybersécurité

Reference number
ISO/PAS 5112:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document is related to ISO/SAE 21434 *Road vehicles — Cybersecurity engineering* and extends ISO 19011 *Guidelines for auditing management systems* to the automotive domain.

This document is intended for organizations involved in automotive cybersecurity engineering in any part of the automotive supply chain and for organizations needing to conduct audits. This document can be used for audits of varying scope.

This document is adapted to fit the scope of an automotive cybersecurity engineering audit programme. Cybersecurity audits in this document are aimed at cybersecurity activities at the organizational level. While results from past projects can be used as evidence for implemented and applied processes, the project and product levels are not in the focus of this document.

This document provides guidelines on the management of an audit programme, on the planning and conducting of management system audits, as well as on the competence and evaluation of an audit team. An audit can be conducted against a range of audit criteria. This document gives a set of audit criteria based on ISO/SAE 21434 objectives. In addition, Annex A contains an example questionnaire that can be adapted.

This document can be used for internal audits (first party), for audits conducted by organizations on their external parties (second party) and for external audits conducted by third parties (e.g. for the purpose of certification). This document can also be useful to organizations involved in auditor training or personnel certification.

Road vehicles — Guidelines for auditing cybersecurity engineering

1 Scope

In addition to the guidelines in ISO 19011, this document provides guidelines to organizations that contribute to the achievement of road vehicle cybersecurity throughout the supply chain on:

- managing an audit programme for a cybersecurity management system (CSMS);
- conducting organizational CSMS audits;
- competencies of CSMS auditors; and
- providing evidence during CSMS audits.

Elements of the CSMS are based on the processes described in ISO/SAE 21434. This document is applicable to those needing to understand or conduct internal or external audits of a CSMS or to manage a CSMS audit programme.

This document does not provide guidelines on cybersecurity assessments.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/SAE 21434:2021, *Road vehicles — Cybersecurity engineering*

ISO 19011:2018, *Guidelines for auditing management systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/SAE 21434, ISO 19011 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
audit
examination of a process to determine the extent to which the process objectives are achieved

Note 1 to entry: “Audit” is defined in ISO 19011 and ISO/SAE 21434. The definition of ISO/SAE 21434 is used in this document to support compatibility between this document and ISO/SAE 21434.

[SOURCE: ISO/SAE 21434:2021, 3.1.6, modified — Note 1 to entry has been added.]

3.2
cybersecurity management system
CSMS
systematic risk-based approach defining organisational processes, responsibilities and governance to manage *risk* (3.3) associated with threats to road vehicles and protect them from threats

[SOURCE: Reference [9], 2.3, modified — added “road” to clarify application domain, replaced “treat” with “manage”, removed “cyber”, replaced “cyber attacks” with “threats”.]

3.3
risk
cybersecurity risk
effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact

Note 1 to entry: ISO 19011 uses a broader definition of the term risk.

[SOURCE: ISO/SAE 21434:2021, 3.1.29, modified — Note 1 to entry has been added.]

3.4
supply chain
set of organizations with a linked set of resources and processes, each of which acts as a customer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement.

Note 1 to entry: A supply chain includes organizations involved in the manufacturing, design and development of vehicles, or service providers involved in the operation, management, and delivery of services.

Note 2 to entry: The supply chain view is relative to the position of the customer.

[SOURCE: ISO/IEC 27036-1:2021, 3.10, modified — “acquirer” replaced by “customer" and Note 1 to entry has been modified.]

4 Principles of auditing

The principles of auditing of ISO 19011:2018, Clause 4 apply. In addition, the following guidance applies.

The guidelines given in this document are aimed at what ISO/SAE 21434 defines as an organizational cybersecurity audit. Product level topics are not in the scope of this document. Regarding products, a cybersecurity assessment based on ISO/SAE 21434 is used to judge the cybersecurity of the item or component.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:2018, 5.1 apply.

5.2 Establishing audit programme objectives

The guidelines of ISO 19011:2018, 5.2 apply. In addition, the following guidance applies.

The audit programme objectives can be based on consideration of the following:

a) demonstration of the achievement of the objectives of ISO/SAE 21434;

b) specific cybersecurity risks associated with the auditee's products;

c) specifics related to the organization’s role in the automotive supply chain; and

EXAMPLE 1 An organization's role can be original equipment manufacturer (OEM), tier 1 supplier, tier 2 supplier, component manufacturer.

NOTE Organizations in the supply chain include organizations which develop components out of context, e.g. before the placement of a purchase order, agreement, or other formal sourcing agreement.

d) clarification of whether the audit includes an evaluation of methods applied in the CSMS processes.

EXAMPLE 2 Specific audit programme objectives can include:

- verification of conformity of the CSMS with relevant legal and contractual requirements;
- obtaining and maintaining confidence in the auditee's CSMS to identify, analyse and evaluate the cybersecurity risk and to take corresponding necessary action; and
- evaluating the effectiveness of the CSMS to address cybersecurity risks.

5.3 Determining and evaluating audit programme risks and opportunities

The guidelines of ISO 19011:2018, 5.3 apply.

5.4 Establishing the audit programme

5.4.1 Roles and responsibilities of the individual(s) managing the audit programme

The guidelines of ISO 19011:2018, 5.4.1 apply.

5.4.2 Competence of individual(s) managing audit programme

The guidelines of ISO 19011:2018, 5.4.2 apply. In addition, the following guidance applies.

The individual(s) managing the CSMS audit programme should have the following competences:

a) knowledge of the standards regarding cybersecurity that are used by the auditee to establish and maintain the CSMS;

b) knowledge of the general processes used by the automotive industry that are relevant for the phase of the cybersecurity lifecycle which is evaluated within the specific scope of the audit (e.g. processes for software development in the automotive domain);

c) ability to map the organization-specific processes, guidelines and rules with the audit criteria; and

d) if a combined audit is conducted, the ability to coordinate with other management system audit programmes.

EXAMPLE A combined audit with IATF 16949[8].

NOTE Considered competence can also include experience in audit or assessment of automotive processes based on automotive standards or guidelines, e.g. IATF 16949 [8], ISO 9001[2], the ISO 26262 series[5], ASPICE[10].

5.4.3 Establishing extent of audit programme

The guidelines of ISO 19011:2018, 5.4.3 apply. In addition, the following guidance applies.

The extent of an audit programme can vary and can be impacted by the following factors:

a) size of the auditee and extent to which the auditee is involved in cybersecurity processes;

b) the cybersecurity-related supply chain and determination of which entities in the supply chain are in scope; and

c) importance of preserving cybersecurity property of information within the scope of the cybersecurity processes.

5.4.4 Determining audit programme resources

The guidelines of ISO 19011:2018, 5.4.4 apply.

5.5 Implementing audit programme

5.5.1 General

The guidelines of ISO 19011:2018, 5.5.1 apply.

5.5.2 Defining the objectives, scope and criteria for an individual audit

The guidelines of ISO 19011:2018, 5.5.2 apply. In addition, the following guidance applies.

The audit scope should include the CSMS processes used by the auditee during the phases of the cybersecurity lifecycle that are within the specific scope of the audit.

EXAMPLE 1 A tier 2 supplier might not be audited for all phases of the cybersecurity lifecycle.

The audit criteria should be defined following 6.4.8 and 6.4.9.

The audit scope may include the whole organization or one or more clearly delineated organizational units.

NOTE 1 Clearly delineated organizational units are those that have separate organizational structures and processes.

If the CSMS process depends on interactions with other organizational processes, the interfaces and dependencies should be identified.

NOTE 2 Interfaces can include how work products are exchanged.

Shared functions outside the organization may be included in the scope of the audit with clearly defined interfaces. If an organization depends on another organization to achieve the objectives of CSMS processes, the contributing organization should be identified. The extent to which the organization manages the dependencies on external organizations to realize its CSMS should be determined.

Distributed cybersecurity activities, defined in a cybersecurity interface agreement, may be included in the scope of the audit.

EXAMPLE 2 Cybersecurity monitoring and cybersecurity incident response.

The audit objectives can include the confirmation of the suitability of the implemented processes and applied methods and criteria to achieve the objectives of ISO/SAE 21434.

The auditee may perform an internal audit to identify and resolve shortcomings in the CSMS before an external audit is conducted. If an external audit is planned as part of the audit programme, the scope and objectives of both internal and external audits should be aligned.

A subsequent follow-up audit to address identified minor non-conformities of a conditionally-passed audit may focus solely on the identified deficiencies noted.

5.5.3 Selecting and determining audit methods

The guidelines of ISO 19011:2018, 5.5.3 apply.

5.5.4 Selecting audit team members

The guidelines of ISO 19011:2018, 5.5.4 apply.

5.5.5 Assigning responsibility for an individual audit to the audit team leader

The guidelines of ISO 19011:2018, 5.5.5 apply.

5.5.6 Managing audit programme results

The guidelines of ISO 19011:2018, 5.5.6 apply.

5.5.7 Managing and maintaining audit programme records

The guidelines of ISO 19011:2018, 5.5.7 apply.

5.6 Monitoring audit programme

The guidelines of ISO 19011:2018, 5.6 apply.

5.7 Reviewing and improving audit programme

The guidelines of ISO 19011:2018, 5.7 apply.

6 Conducting an audit

6.1 General

The guidelines of ISO 19011:2018, 6.1 apply.

6.2 Initiating audit

6.2.1 General

The guidelines of ISO 19011:2018, 6.2.1 apply.

6.2.2 Establishing contact with auditee

The guidelines of ISO 19011:2018, 6.2.2 apply. In addition, the following guidance applies.

Auditor and auditee should mutually agree on information that is not to be disclosed.

Information can be classified as confidential and sensitive. Access to such information can be limited to selected audit team members.

EXAMPLE Documents can only be viewed in an area controlled by the auditee. Transfer and processing of the documents outside this environment is prohibited.

6.2.3 Determining feasibility of audit

The guidelines of ISO 19011:2018, 6.2.3 apply.

6.3 Preparing audit activities

6.3.1 Performing review of documented information

The guidelines of ISO 19011:2018, 6.3.1 apply.

6.3.2 Audit planning

6.3.2.1 Risk-based approach to planning

The guidelines of ISO 19011:2018, 6.3.2.1 apply.

6.3.2.2 Audit planning details

The guidelines of ISO 19011:2018, 6.3.2.2 apply. In addition, the following guidance applies.

The audit should be planned to address the corresponding objectives of ISO/SAE 21434 by means of a questionnaire.

NOTE See Annex A for an example questionnaire.

6.3.3 Assigning work to audit team

The guidelines of ISO 19011:2018, 6.3.3 apply.

6.3.4 Preparing documented information for audit

The guidelines of ISO 19011:2018, 6.3.4 apply.

6.4 Conducting audit activities

6.4.1 General

The guidelines of ISO 19011:2018, 6.4.1 apply.

6.4.2 Assigning roles and responsibilities of guides and observers

The guidelines of ISO 19011:2018, 6.4.2 apply.

6.4.3 Conducting opening meeting

The guidelines of ISO 19011:2018, 6.4.3 apply. In addition, the following guidance applies.

The audit team and the auditee should agree on:

a) information and/or material types and dissemination of the information to the audit team, location of the information and/or materials, other evidences;

b) the procedure to add audit team members on an ad-hoc basis;

c) auditing processes and methods of auditing the supply-chain partners (outsourced partners);

d) the method of communication on an ad-hoc basis; and

e) availability and access to required information.

6.4.4 Communicating during audit

The guidelines of ISO 19011:2018, 6.4.4 apply. In addition, the following guidance applies.

The audit team and auditee should communicate regarding:

a) deviation from audit approaches or methods;

b) deviation from expectations with respect to the objectives of the audit program;

c) deviation from the point of contact availability;

d) deviation from declared communication procedure;

e) absence of evidence or documentation due to the confidentiality and/or sensitivity of the evidence or documentation during the audit;

f) deviation from declared organizational cybersecurity processes; and

g) cybersecurity risks encountered during the audit.

6.4.5 Audit information availability and access

The guidelines of ISO 19011:2018, 6.4.5 apply. In addition, the following guidance applies.

Relevant third party, partner, supplier, and stakeholder information should be provided, if such information can be shared.

Request for access to confidential information should be justified including an explanation of the need regarding scope and depth of the requested information.

NOTE Audit information availability and access are included in 6.2.2 regarding the planning of information access, in 6.4.4 for the communication of unavailable information during the audit and in 6.6 regarding the handling of information access for auditors in the completion of an audit.

If any audit evidence is unavailable to the audit team during the audit due to confidentiality and/or sensitivity, the audit team leader should:

- determine the extent to which this affects the confidence in the audit findings and conclusion; and
- reflect this in the audit report without compromising the sensitivity of the unavailable evidence.

6.4.6 Reviewing documented information while conducting audit

The guidelines of ISO 19011:2018, 6.4.6 apply.

6.4.7 Collecting and verifying information

The guidelines of ISO 19011:2018, 6.4.7 apply. In addition, the following guidance applies.

Methods to collect relevant information during the audit can include:

a) review of documented information on policy and rules on the engineering of items and components;

b) observation of cybersecurity processes and methods; and

EXAMPLE Project related work products.

c) observation of engineering environment.

6.4.8 Generating audit findings

The guidelines of ISO 19011:2018, 6.4.8 apply. In addition, the following guidance applies.

Findings should be graded based on the guidance in Table 1 by conformity or nonconformity to objectives instead of quantitative gradations.

Table 1 — Criteria for grading of findings

Criteria	Grade
Objective evidence regarding full achievement of all objectives	Conformity
Minor deviations were observed.	Minor nonconformity
Major deviations were observed, one or more objectives are not achieved.	Major nonconformity

A rationale should be provided for all unfulfilled audit criteria that leads to nonconformity.

6.4.9 Determining audit conclusions

The guidelines of ISO 19011:2018, 6.4.9 apply. In addition, the following guidance applies.

The conclusion of the audit should be derived out of the grading of all findings in accordance with the criteria defined in Table 2.

Table 2 — Criteria for deriving overall audit conclusions

Criteria	Audit conclusion
There are no major nonconformities and no minor nonconformities.	Pass
There is one or more minor nonconformities, but no major nonconformities. Identified minor nonconformities do not call into question the overall effectiveness of the CSMS.	Conditional pass
One or more major nonconformities or several minor nonconformities that, due to their number or in their dependencies, call into question the overall effectiveness of the CSMS.	Fail

For a failed or conditionally passed audit, corrective actions should be defined. The auditee should analyse the root causes and specify corrective measures.

For a conditionally passed audit, if the corrective actions are not provided by the auditee or not accepted by the audit team, the audit conclusion should be a fail.

6.4.10 Conducting closing meeting

The guidelines of ISO 19011:2018, 6.4.10 apply.

6.5 Preparing and distributing audit report

6.5.1 Preparing audit report

The guidelines of ISO 19011:2018, 6.5.1 apply.

6.5.2 Distributing audit report

The guidelines of ISO 19011:2018, 6.5.2 apply. In addition, the following guidance applies.

Appropriate measures to ensure the confidentiality and integrity of the audit report should be applied.

EXAMPLE 1 Use of appropriate encryption to ensure confidentiality.

EXAMPLE 2 Use of digital signatures to ensure and validate integrity.

6.6 Completing audit

The guidelines of ISO 19011:2018, 6.6 apply. In addition, the following guidance applies.

If documented information pertaining to the audit are retained by the audit team, an agreement should be established between the audit team and the auditee for the treatment of information classified as confidential.

NOTE 1 This can include notes that contain sensitive information.

If disclosure to a third party of any information obtained during the audit is required, an agreement should be established between the audit team and the auditee for the disclosure.

If the auditee provides access to confidential information, then the audit team should inform the auditee when access is no longer required so that access can be revoked. For subsequent follow-up activities, access may be re-granted for the duration of the follow-up activity.

Information classified as confidential should be used only for lessons learned based on an agreement between participating parties.

NOTE 2 Notes taken during the audit can be considered for completing the audit.

6.7 Conducting audit follow-up

The guidelines of ISO 19011:2018, 6.7 apply. In addition, the following guidance applies.

Inclusion of confidential information in reporting status and results of follow up activities should be based on an agreement between auditee and audit team.

7 Competence and evaluation of auditors

7.1 General

The guidelines of ISO 19011:2018, 7.1 apply.

7.2 Determining auditor competence

7.2.1 General

The guidelines of ISO 19011:2018, 7.2.1 apply. In addition, the following guidance applies.

In deciding the necessary competence of an auditor, the following should be considered:

a) standards, legal requirements and other requirements relevant to the audit programme; and

b) dependencies between the CSMS and other management systems.

EXAMPLE Information security management system (ISMS), software update management system (SUMS).

7.2.2 Personal behaviour

The guidelines of ISO 19011:2018, 7.2.2 apply.

7.2.3 Knowledge and skills

7.2.3.1 General

The guidelines of ISO 19011:2018, 7.2.3.1, apply.

7.2.3.2 Generic knowledge and skills of management system auditors

The guidelines of ISO 19011:2018, 7.2.3.2, apply.

7.2.3.3 Discipline and sector specific competence of auditors

The guidelines of ISO 19011:2018, 7.2.3.3 apply. In addition, the following guidance applies.

The audit team should have knowledge and skills in:

a) automotive technologies;

NOTE 1 See B.4 for examples.

b) cybersecurity processes, in particular road-vehicle cybersecurity and corresponding risk management (to evaluate the methods used by the auditee);

c) cybersecurity management systems (to evaluate the effectiveness of the cybersecurity processes for, e.g. cybersecurity control determination planning implementation, maintenance and effectiveness of the cybersecurity processes); and

d) ISO/SAE 21434.

NOTE 2 See B.2 for examples.

EXAMPLE Evidence of competence can be demonstrated through education, training or overall working experience in the fields of automotive industry, cybersecurity, and technology relevant for the auditee.

7.2.3.4 Generic competence of audit team leader

The guidelines of ISO 19011:2018, 7.2.3.4, apply.

7.2.3.5 Knowledge and skills for auditing multiple disciplines

The guidelines of ISO 19011:2018, 7.2.3.5, apply.

7.2.4 Achieving auditor competence

The guidelines of ISO 19011:2018, 7.2.4 apply.

7.2.5 Achieving audit team leader competence

The guidelines of ISO 19011:2018, 7.2.5 apply.

7.3 Establishing auditor evaluation criteria

The guidelines of ISO 19011:2018, 7.3 apply.

7.4 Selecting appropriate auditor evaluation method

The guidelines of ISO 19011:2018, 7.4 apply.

7.5 Conducting auditor evaluation

The guidelines of ISO 19011:2018, 7.5 apply.

7.6 Maintaining and improving auditor competence

The guidelines of ISO 19011:2018, 7.6 apply.

Annex A
(informative)

Audit questionnaire

A.1 General

This annex gives an example of a questionnaire that the audit team can refer to as indicators for implementing the shown objectives of ISO/SAE 21434:2021. This questionnaire can be extended or customized as needed. Work products as defined in ISO/SAE 21434:2021 can be considered as supporting documents for implementation of the required processes. The absence of these work products is not evidence that the process is non-existent or inadequate. Other appropriate evidences can also be considered as implementation of the required processes. To pass the audit, the audit team should receive from the auditee evidence regarding achievement of the objectives defined for each audit question in this annex. Evidence examples given in A.2 refer to both process specifications and samples of project-related work products of the performed process.

NOTE References to work products ([WP-XX-YY]) in evidence examples refer to work products defined in ISO/SAE 21434:2021.

A.2 Audit questionnaire

A.2.1 Cybersecurity management

Q1.1 Are cybersecurity policy, rules and processes defined?	
ISO/SAE 21434 Objectives	5.2 a) define a cybersecurity policy and the organization-specific rules and processes for cybersecurity.
Guidelines for the auditor	Auditors should verify that: — the cybersecurity policy and the organization-specific rules and processes for cybersecurity are defined; and — the cybersecurity policy in this organization commits to managing cybersecurity risk related to the organization’s activities.
Evidence examples	— [WP-05-01] Cybersecurity policy, rules and processes

Q1.2 Are cybersecurity-relevant processes managed?	
ISO/SAE 21434 Objectives	5.2 b) assign the responsibilities and corresponding authorities that are required to perform cybersecurity activities; 5.2 c) support the implementation of cybersecurity, including the provision of resources and the management of the interactions between cybersecurity processes and related processes; 5.2 d) manage the cybersecurity risk; 5.2 f) support and manage the sharing of cybersecurity information; 5.2 g) institute and maintain management systems that support the cybersecurity; 5.2 h) provide evidence that the use of tools does not adversely affect cybersecurity; and 5.2 i) perform an organizational cybersecurity audit.

Q1.2	Are cybersecurity-relevant processes managed?
Guidelines for the auditor	Auditors should verify that: — the organization invests resources to manage the cybersecurity risks; — the organization assigns and communicates the responsibilities to achieve and maintain cybersecurity for the relevant phases of the product lifecycle and grants the corresponding authorization while providing required resources; — the organization manages cybersecurity risks; — the organization has defined the circumstances under which sharing of cybersecurity information is required, permitted, and prohibited, within and outside of the organization; — the organization institutes and maintains a quality management system in accordance with international standards, or equivalent, to support cybersecurity engineering; and — the organization manages tools that can impact the cybersecurity of an item, or component.
Evidence examples	— [WP-05-01] Cybersecurity policy, rules and processes — [WP-05-03] Evidence of organization’s management systems — [WP-05-04] Evidence of tool management — [WP-05-05] Organizational cybersecurity audit report

Q1.3	Are cybersecurity culture and cybersecurity awareness established, implemented, and maintained?
ISO/SAE 21434 Objectives	5.2 e) institute and maintain a cybersecurity culture, including competence management, awareness management and continuous improvement.
Guidelines for the auditor	Auditors should verify that: — personnel have the competences and awareness to fulfil their responsibilities through demonstratable experience, awareness and training programmes; and — the organization has defined processes for competence management, awareness management, and continuous improvement. EXAMPLE Continuous improvements can include: a) learning from previous cybersecurity experiences, including experiences gathered by field monitoring and observation of internal and external information; b) learning from information obtained regarding products of similar application in the field; c) deriving improvements to be applied during subsequent cybersecurity activities; d) communicating lessons learned to the appropriate persons; and e) regularly checking the adequacy of its rules and processes.
Evidence examples	— [WP-05-02] Evidence of competence management, awareness management and continuous improvement

Q1.4	Is a process established, implemented, and maintained to manage project dependent cybersecurity?
ISO/SAE 21434 Objectives	6.2 b) plan the cybersecurity activities, including the definition of the tailored cybersecurity activities; 6.2 c) create a cybersecurity case; and 6.2 d) perform a cybersecurity assessment, if applicable.
Guidelines for the auditor	Auditors should verify that: — a process is established for the creation of a cybersecurity plan; — a process is established for the creation of a cybersecurity case; and — a process is established for a cybersecurity assessment.
Evidence examples	— [WP-06-01] Cybersecurity plan — [WP-06-02] Cybersecurity case — [WP-06-03] Cybersecurity assessment report

A.2.2 Continual cybersecurity activities

Q2.1	Is a process established, implemented, and maintained to monitor for cybersecurity information?
ISO/SAE 21434 Objectives	8.2 a) monitor cybersecurity information to identify cybersecurity events.
Guidelines for the auditor	Auditors should verify that: — a process is established, that checks sources of cybersecurity information for new cybersecurity information relevant to the organization's items and components; and — a process for triage is established that determines if newly obtained cybersecurity information results in a cybersecurity event.
Evidence examples	— [WP-08-01] Sources for cybersecurity information — [WP-08-02] Triggers — [WP-08-03] Cybersecurity events

Q2.2	Is a process established, implemented, and maintained to evaluate cybersecurity events?
ISO/SAE 21434 Objectives	8.2 b) evaluate cybersecurity events to identify weaknesses.
Guidelines for the auditor	Auditors should verify that: — a process is established to evaluate cybersecurity events to identify weaknesses in an organization's items or components.
Evidence examples	— [WP-08-04] Weaknesses from cybersecurity events

Q2.3	Is a process established, implemented, and maintained to identify and analyse vulnerabilities?
ISO/SAE 21434 Objectives	8.2 c) identify vulnerabilities from weaknesses; and 10.2 c) identify weaknesses in the component.
Guidelines for the auditor	Auditors should verify that: — a process is established that analyses weaknesses to identify vulnerabilities.
Evidence examples	— [WP-08-05] Vulnerability analysis

Q2.4 Is a process established, implemented, and maintained to manage identified vulnerabilities?	
ISO/SAE 21434 Objectives	8.2 d) manage identified vulnerabilities.
Guidelines for the auditor	Auditors should verify that: — a process is established to manage identified vulnerabilities, including risk determination and risk treatment.
Evidence examples	— [WP-08-06] Evidence of managed vulnerabilities

A.2.3 Risk assessment and methods

Q3.1 Are methods established, implemented, and maintained to determine cybersecurity risks for an item across concept, product development and post-development phases?	
ISO/SAE 21434 Objectives	15.2 c) determine the impact rating of damage scenarios; 15.2 e) determine the ease with which attack paths can be exploited; and 15.2 f) determine the risk values of threat scenarios.
Guidelines for the auditor	Auditors should verify that: — the organization has defined criteria for rating the impacts in different impact categories; — the organization has defined a method for rating the attack feasibility for identified attack paths; and — the organization has defined a method for risk value determination.
Evidence examples	— [WP-15-04] Impact ratings with associated impact categories — [WP-15-06] Attack feasibility ratings — [WP-15-07] Risk values

Q3.2 Is a process established, implemented, and maintained to perform a threat analysis and risk assessment (TARA) for an item across concept, product development and post-development phases?	
ISO/SAE 21434 Objectives	15.2 a) identify assets, their cybersecurity properties and their damage scenarios; 15.2 b) identify threat scenarios; 15.2 c) determine the impact rating of damage scenarios; 15.2 d) identify the attack paths that realize threat scenarios; 15.2 e) determine the ease with which attack paths can be exploited; 15.2 f) determine the risk values of threat scenarios; and 15.2 g) select the appropriate risk treatment options for threat scenarios.
Guidelines for the auditor	Auditors should verify that: — a process is established for performing a threat analysis and risk assessment (TARA) for an item across concept, product development, and post-development phases; and — a process is established to determine a risk treatment option considering impact categories, attack paths and the results from risk value determination across concept, product development and post-development phases.

Q3.2 Is a process established, implemented, and maintained to perform a threat analysis and risk assessment (TARA) for an item across concept, product development and post-development phases?	
Evidence examples	— [WP-15-01] Damage scenarios — [WP-15-02] Assets with cybersecurity properties — [WP-15-03] Threat scenarios — [WP-15-04] Impact ratings with associated impact categories — [WP-15-05] Attack paths — [WP-15-06] Attack feasibility ratings — [WP-15-07] Risk value — [WP-15-08] Risk treatment decisions

Q3.3 Is a process established, implemented, and maintained to treat cybersecurity risks for the item across concept, product development and post-development phases?	
ISO/SAE 21434 Objectives	9.2 b) specify cybersecurity goals and cybersecurity claims; and 15.2 g) select the appropriate risk treatment options for threat scenarios.
Guidelines for the auditor	Auditors should verify that: — a process is established to treat cybersecurity risks, including the specification of cybersecurity goals and cybersecurity claims.
Evidence examples	— [WP-09-04] Cybersecurity claims — [WP-09-03] Cybersecurity goals — [WP-09-02] TARA result

A.2.4 Concept and product development phase

Q4.1 Is a process established, implemented, and maintained to define the item and specify cybersecurity requirements?	
ISO/SAE 21434 Objectives	9.2 a) define the item, its operational environment and their interaction in the context of cybersecurity; 9.2 b) specify cybersecurity goals and cybersecurity claims; and 9.2 c) specify the cybersecurity concept to achieve cybersecurity goals.
Guidelines for the auditor	Auditors should verify that: — a process is established for item definition; and — a process is established for specification and verification of cybersecurity requirements.

Q4.1 Is a process established, implemented, and maintained to define the item and specify cybersecurity requirements?	
Evidence examples	— [WP-09-01] Item definition — [WP-09-02] TARA — [WP-09-03] Cybersecurity goals — [WP-09-04] Cybersecurity claims — [WP-09-05] Verification report for cybersecurity goals — [WP-09-06] Cybersecurity concept — [WP-09-07] Verification report for the cybersecurity concept

Q4.2 Is a process established, implemented, and maintained for verification of cybersecurity requirements on components during the development phase?	
ISO/SAE 21434 Objectives	10.2 b) verify that the defined cybersecurity specifications conform to the cybersecurity specifications from higher levels of architectural abstraction; and 10.2 d) provide evidence that the results of the implementation and integration of components conform to the cybersecurity specifications.
Guidelines for the auditor	Auditors should verify that: — a process is established for verification of cybersecurity specification.
Evidence examples	— [WP-10-04] Verification report for the cybersecurity specifications — [WP-10-05] Weakness found during product development, if applicable — [WP-10-06] Integration and verification specification — [WP-10-07] Integration and verification report

Q4.3 Is a process established, implemented, and maintained for validation of cybersecurity goals and claims at an item level?	
ISO/SAE 21434 Objectives	11.2 a) validate the cybersecurity goals and cybersecurity claims; 11.2 b) confirm the item achieves the cybersecurity goals; and 11.2 c) confirm that no unreasonable risks remain.
Guidelines for the auditor	Auditors should verify that: — a process is established for validation of cybersecurity goals and claims.
Evidence examples	— [WP-11-01] Validation report

A.2.5 Post-development phase

Q5.1 Is there a process established, implemented, and maintained for release of an item or component for post development phases?	
ISO/SAE 21434 Objectives	6.2 e) decide whether the item or component can be released for post-development from a cybersecurity perspective.