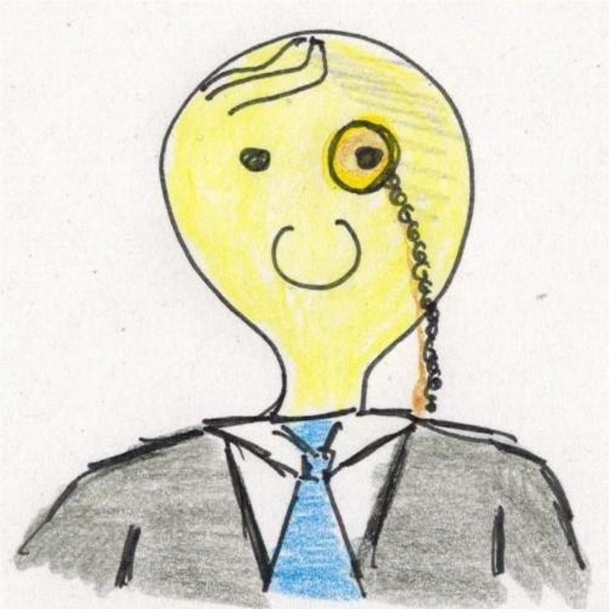
Cybersecurity: Audit or Assessment?

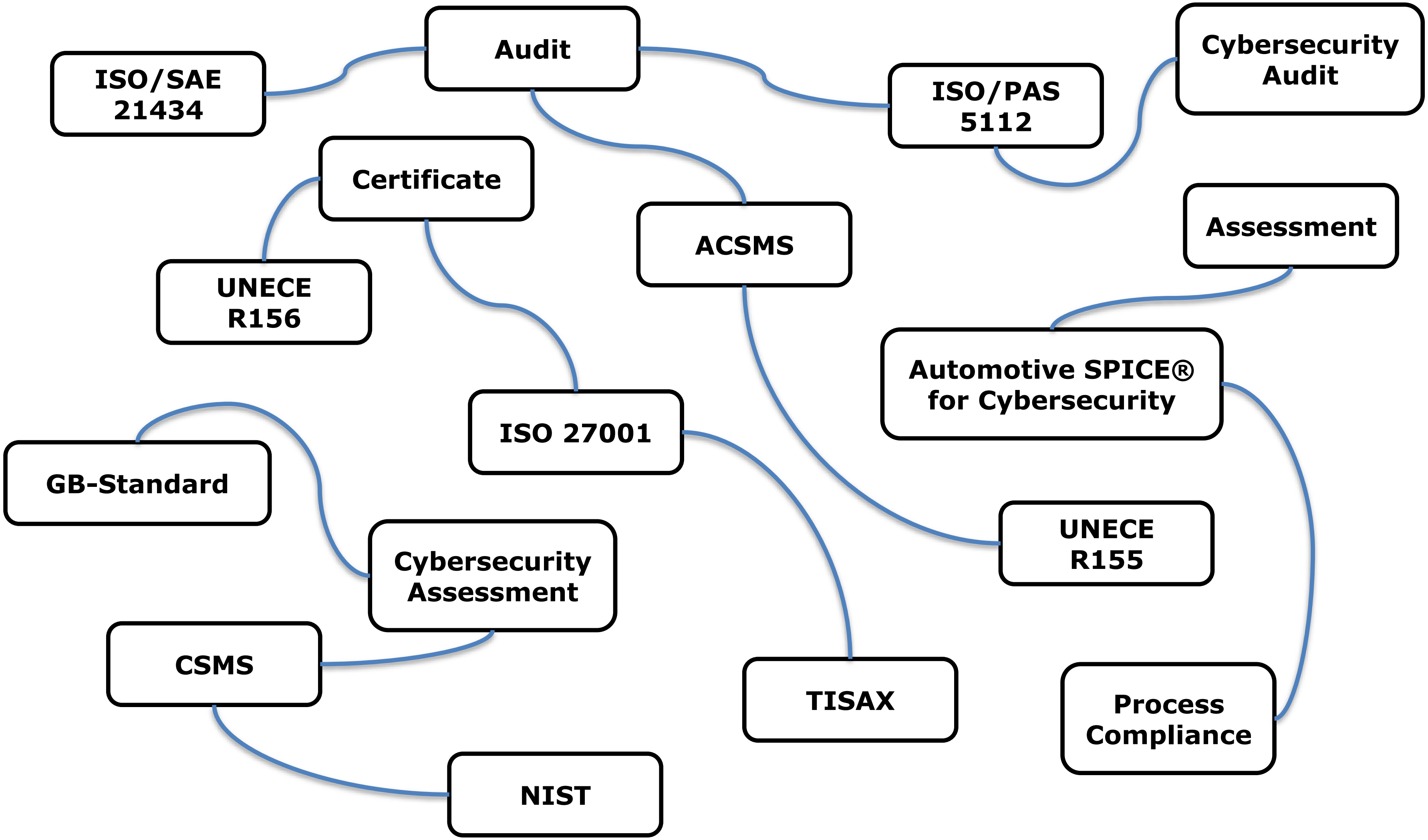


Webinar

Timo Karasch

September 23rd, 2025

Motivation



Audit

ISO/SAE 21434

ISO/PAS 5112

Cybersecurity Audit

Certificate

ACSMS

Assessment

UNECE R156

Automotive SPICE® for Cybersecurity

ISO 27001

GB-Standard

UNECE R155

Cybersecurity Assessment

CSMS

TISAX

Process Compliance

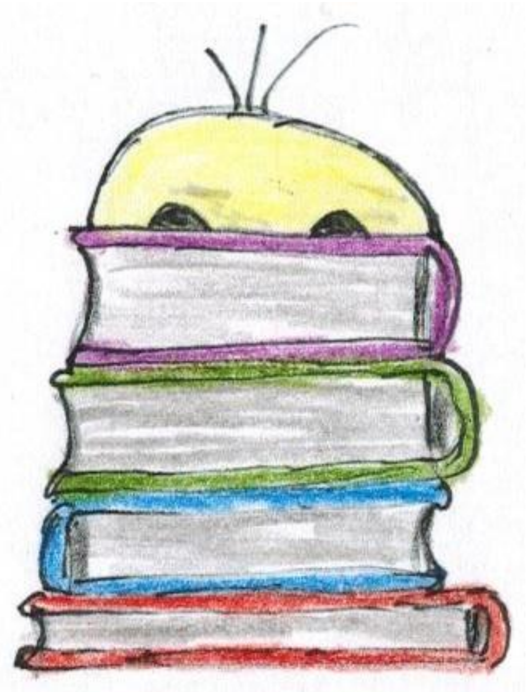
NIST

Agenda

1. What are Audits and Assessments?
2. What is the purpose of those standards?

3. Measures in ISO/SAE 21434
4. Measures in ACSMS
5. Measures in ISO/PAS 5112
6. Measures in Automotive SPICE® for Cybersecurity
7. Measures in UNECE R155

8. Recommendation for Suppliers



1. What are Audits and Assessments?
In ISO/SAE 21434

[cybersecurity] audit

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

[SOURCE: ISO 26262-1:2018]

In ISO/SAE 21434 used for "Organizational Audit", but in ISO 26262 in "Project dependent confirmation measure"

≠

An **ISO 9000** audit is a planned review of a quality management system to ensure that it meets the requirements and to identify potential for improvement.

[cybersecurity] assessment

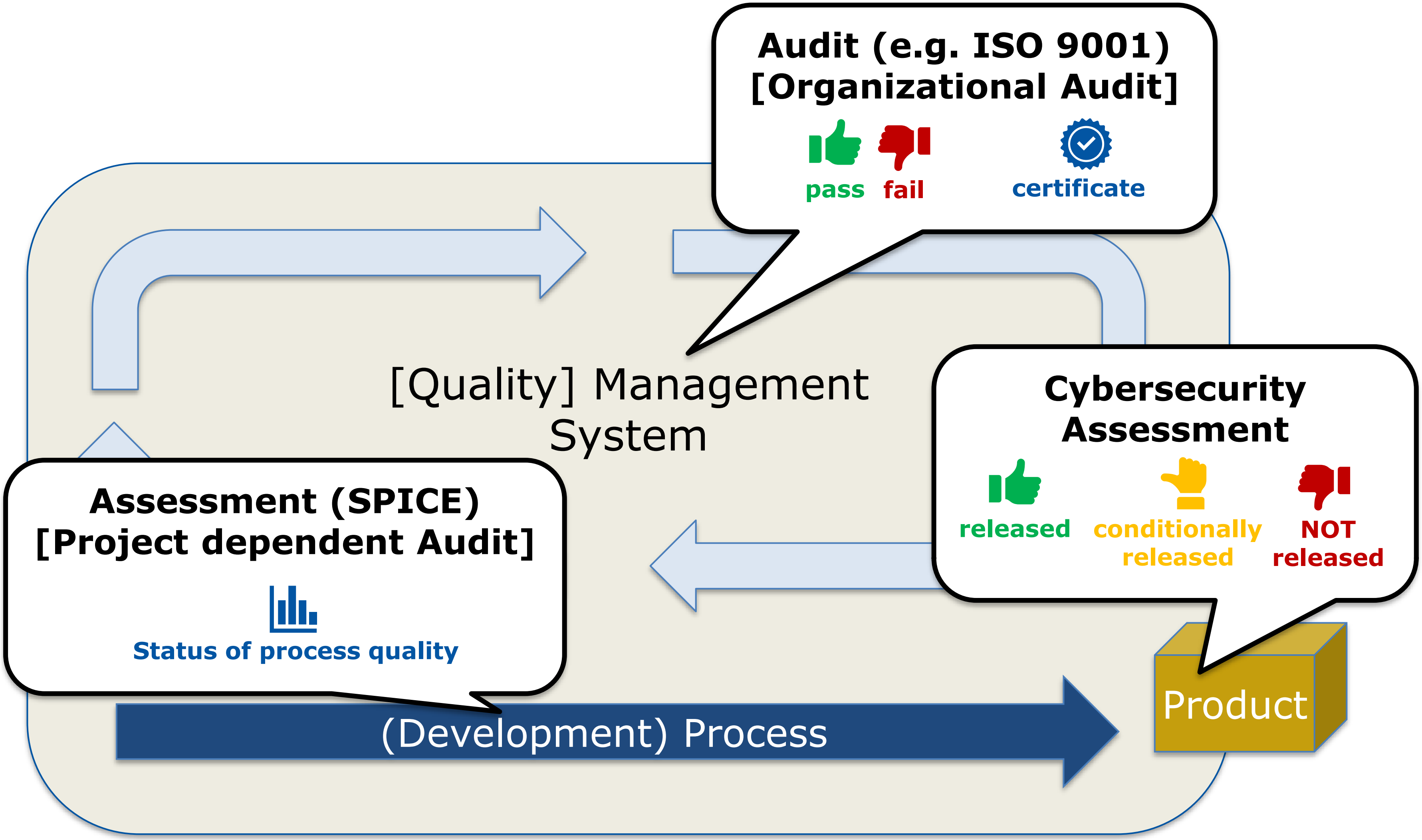
judgement of *cybersecurity*

[or in ISO 26262-1:2018: examination of whether a characteristic of an *item* or *element* achieves the ISO 26262 objectives]

≠

A **SPICE** assessment demonstrates that processes are not only implemented but also consistently applied, leading to higher product quality and customer satisfaction.

1. What are Audits and Assessments?
What does this mean?



Audit (e.g. ISO 9001)
[Organizational Audit]

pass fail certificate

[Quality] Management System

Cybersecurity Assessment

released conditionally released NOT released

Assessment (SPICE)
[Project dependent Audit]

Status of process quality

(Development) Process

Product

2. What is the purpose of those standards?

International Standard

ISO 27001
It helps companies comprehensively protect their information assets—from data and systems to employees.

ISO/SAE 21434
The standard provides a structured framework for assessing threats, identifying risks, and implementing risk mitigation measures.

ISO/PAS 5112
Helps organizations assess the impact of cybersecurity on their processes and ensure compliance with ISO/SAE 21434

Europe

UNECE R155
Manufacturers must demonstrate a comprehensive cybersecurity risk management system based on the entire vehicle lifecycle.

UNECE R156
Vehicle manufacturers are responsible for introducing and operating a SUMS that complies with standards and must demonstrate its conformity.

VDA

ACSMS
Cybersecurity Management System with focus on the specifics in the automotive sector.

Automotive SPICE® for Cybersecurity
The CS PAM supplements the core Automotive SPICE PAM to incorporate cybersecurity-specific processes into the established evaluation framework.

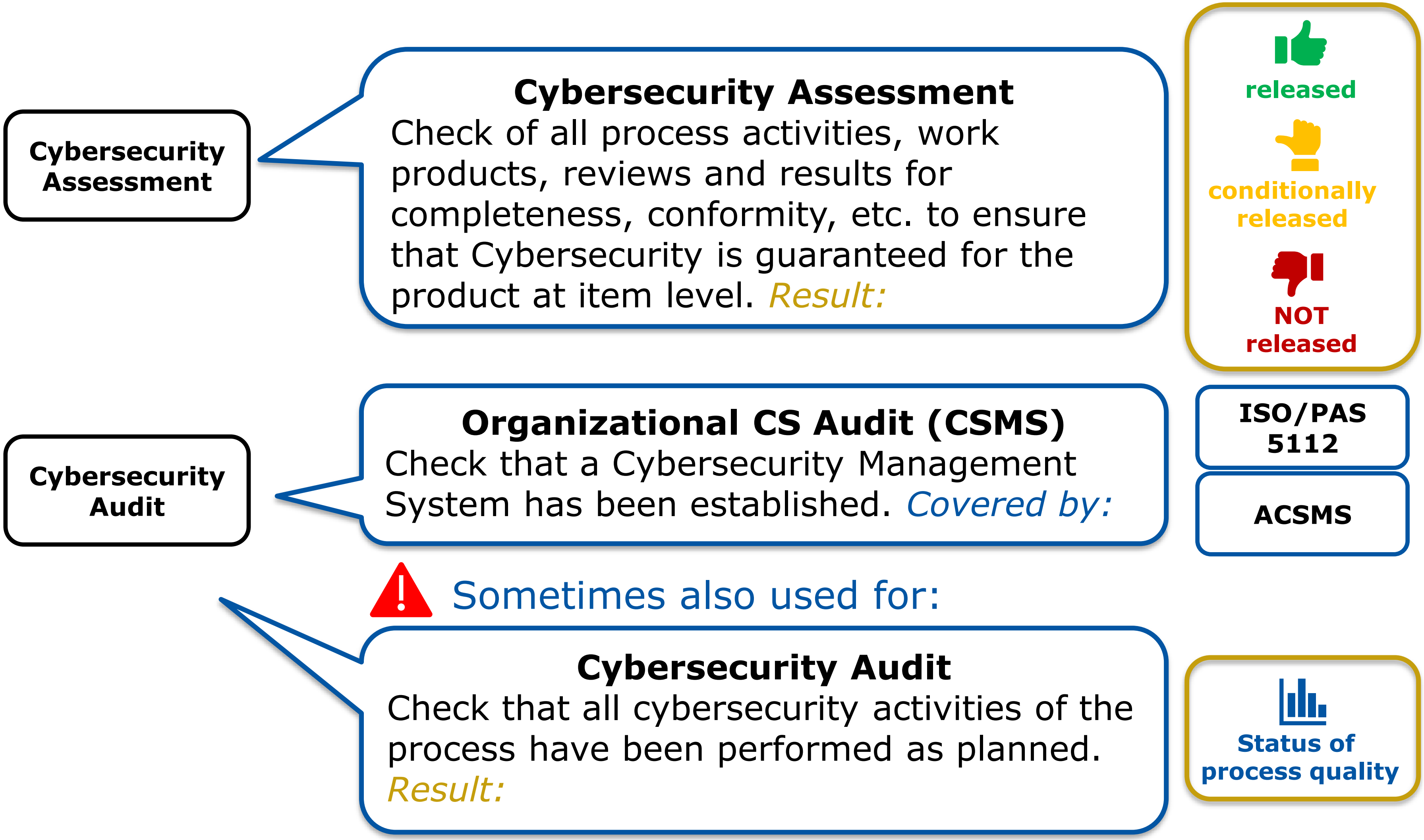
other

TISAX
Companies in the automotive industry can demonstrate their information security, which reduces effort and multiple audits.

NIST
The NIST Cybersecurity Framework is a recognized, voluntary guideline for companies worldwide to manage their cybersecurity risks and protect their systems.

GB-Standard
They ensure product safety, promote fair competition, and support technological advancement and innovation in China.

3. Measures in ISO/SAE 21434



Cybersecurity Assessment

Cybersecurity Assessment
Check of all process activities, work products, reviews and results for completeness, conformity, etc. to ensure that Cybersecurity is guaranteed for the product at item level. *Result:*

👍 **released**

conditionally released

👎 **NOT released**

Cybersecurity Audit

Organizational CS Audit (CSMS)
Check that a Cybersecurity Management System has been established. *Covered by:*

ISO/PAS 5112

ACSMS

⚠ Sometimes also used for:

Cybersecurity Audit
Check that all cybersecurity activities of the process have been performed as planned.
Result:

Status of process quality

4. Measures in ACSMS

Audit

Audit of CSMS

Check that a Cybersecurity Management System has been established (at OEM and supplier site). This is based on the requirements of the UNECE R155.
It defines an (exemplary) questionnaire for the audit, as well as requirements for auditors. *Result:*

👍 passed

👉 Failed With measures

👎 failed

⚠ The certificate is often a requirement by OEMs!

👆 As known from other VDA standards it defines „questions" and „relevant minimum requirements" for CS management, risk identification, Risk assessment, categorization and management, Consistency check, Updating the risk assessment, CS incident response, Reporting against authorities and CS management in the supply chain.

5. ISO/PAS 5112

Audit

Audit of CSMS

Check that a Cybersecurity Management System has been established (at OEM and supplier site). This is based on the requirements of the ISO/SAE 21434.
It defines an (exemplary) questionnaire for the audit, as well as requirements for the audit process (based on ISO 19011) and auditors. *Result:*

👍 **pass**

✋ **Conditional pass**

👎 **fail**

⚠ The certificate is often a requirement by OEMs. It can be seen as an alternative to ACSMS!

☝ It defines „objective", „guidelines" and „exemplary evidences" for CS management, Continual CS activities, Risk assessment and methods, Concept and product development phase, Post-development phase and Distributed CS activities.

6. Measures in Automotive SPICE® for Cybersecurity

Automotive SPICE® Assessment

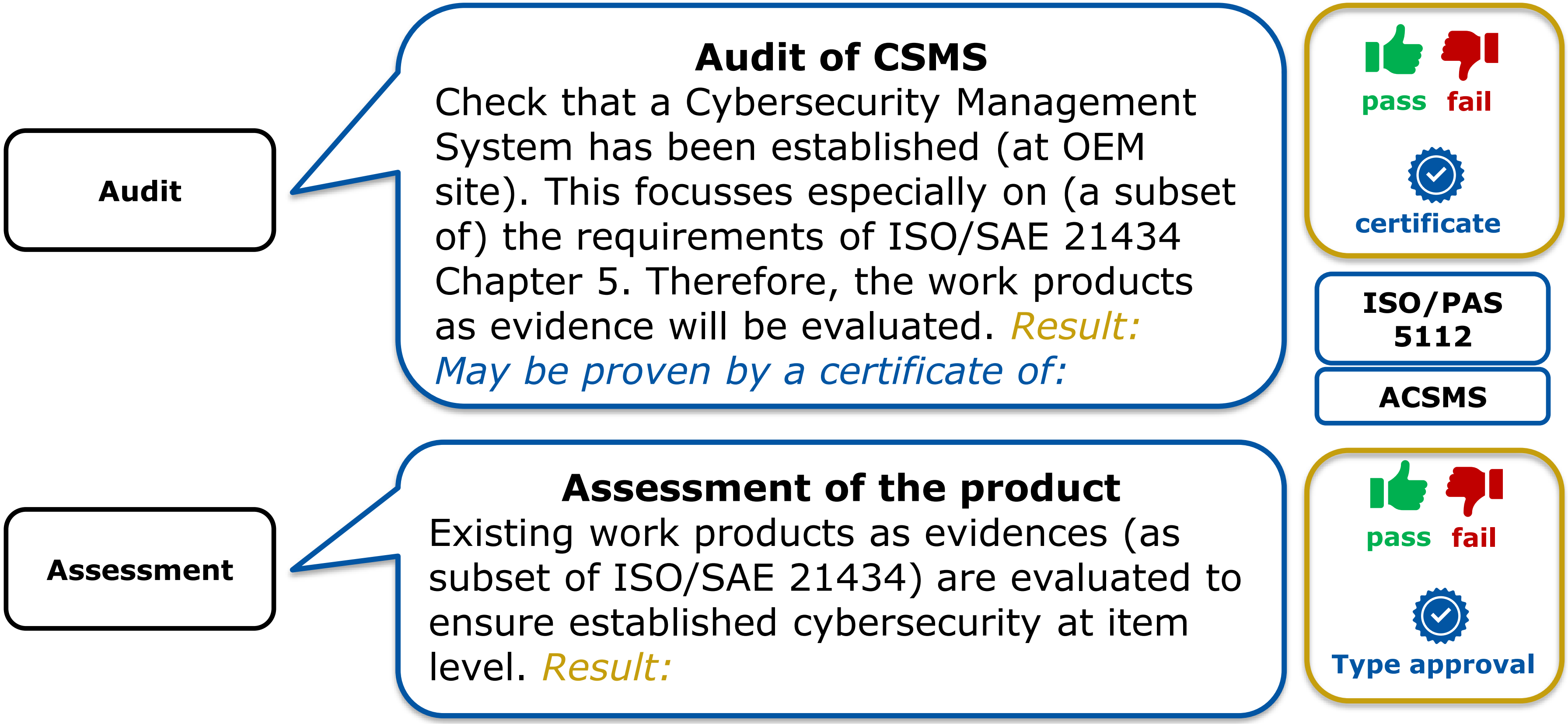
Automotive SPICE® for Cybersecurity Assessment
„Combined" OR „Add-on"

Evaluation of the development processes for the entire system either „combined" (System + Hardware + Software + Cybersecurity development) or as „add-on" (Cybersecurity development based on an existing Automotive SPICE® Assessment).
Goals are to identify process improvements and to determine the capability of the used processes. *Result:*

Status of process quality

⚠ The coverage of project-specific cybersecurity management activities depends on the target level and the assessor education!

7. Measures in UNECE R155



Audit

Audit of CSMS

Check that a Cybersecurity Management System has been established (at OEM site). This focusses especially on (a subset of) the requirements of ISO/SAE 21434 Chapter 5. Therefore, the work products as evidence will be evaluated. *Result: May be proven by a certificate of:*

pass fail

certificate

ISO/PAS 5112

ACSMS

Assessment

Assessment of the product

Existing work products as evidences (as subset of ISO/SAE 21434) are evaluated to ensure established cybersecurity at item level. *Result:*

pass fail

Type approval

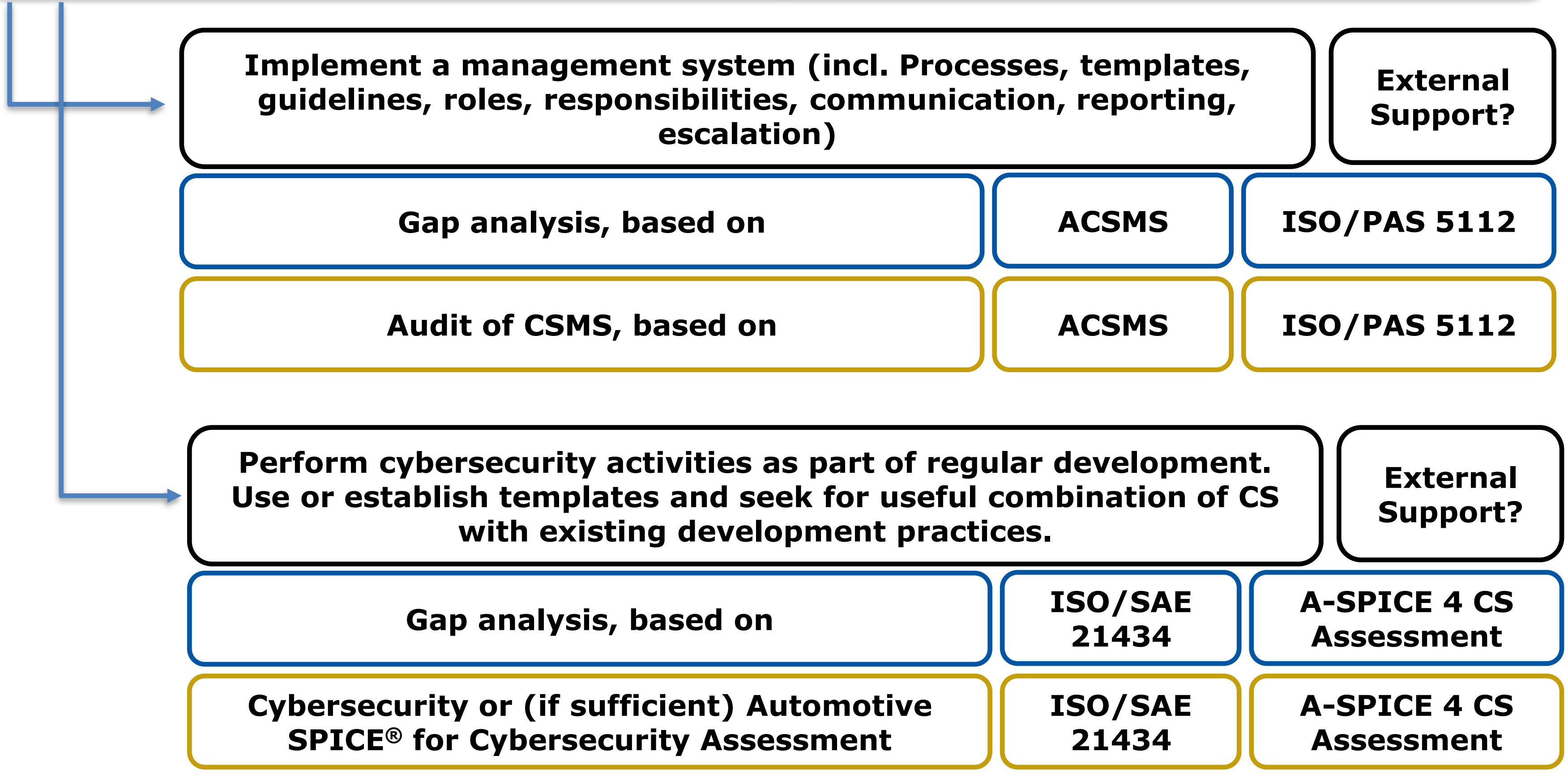
This is mandatory only on OEM level!

The annex of this standard often is used as required source for TARA at supplier site.

8. Recommendation for Suppliers

Customer (OEM) requirements [typically]:

- Provide certificate of a CSMS
- Ensure development according to ISO/SAE 21434



Implement a management system (incl. Processes, templates, guidelines, roles, responsibilities, communication, reporting, escalation)

External Support?

Gap analysis, based on | **ACSMS** | **ISO/PAS 5112**

Audit of CSMS, based on | **ACSMS** | **ISO/PAS 5112**

Perform cybersecurity activities as part of regular development. Use or establish templates and seek for useful combination of CS with existing development practices.

External Support?

Gap analysis, based on | **ISO/SAE 21434** | **A-SPICE 4 CS Assessment**

Cybersecurity or (if sufficient) Automotive SPICE® for Cybersecurity Assessment | **ISO/SAE 21434** | **A-SPICE 4 CS Assessment**

Thank you!

Process Fellows GmbH | Schlegelleithe 8 | 91320 Ebermannstadt | GERMANY
Phone: +49 9194 3719 957 | Fax: +49 9194 3719 – 579
Website: www.processfellows.de | E-Mail: info@processfellows.de