DNV

ISACA
Barcelona Chapter

TISAX®

Transformando la Seguridad en la industria de Automoción

Alex Komlev

24 April 2024

TISAX®

Transformando la Seguridad en la industria de Automoción

Alex Komlev

24 April 2024

Agenda

Item	Topic
	Welcome
01	TISAX® Introduction
02	Main goals
03	TISAX® VDA structure
04	TISAX® vs ISO27001
05	5 reasons why company should get TISAX®
06	Basic documents
07	Certification process
08	Assessment process
09	VDA ISA Catalogue
10	Recap
	Q&A

+34-647128056

Alexey.Komlev@dnv.com

Alex Komlev

ICT Global Technical Hub Manager

DNV © 2021

What is TISAX®?

Basic introduction.

Trusted Information Security Assessment Exchange

- TISAX is an assessment and exchange mechanism for information security in the automotive industry. The TISAX label confirms that a company's information security management system complies with defined security levels and allows sharing of assessment results across a designated platform.

- The Original Equipment Manufacturer (**OEM**) collaborates with multiple companies across the value chain for the design, manufacturing, and distribution of their vehicles. To facilitate collaboration, the OEM frequently shares confidential information, such as a ***prototype*** design, with the suppliers. If valuable data is not effectively protected, the exchanges along the supply chain may cause losses, manipulations or even theft of trade secrets.

- The TISAX scheme is based on the international standard **ISO 27001**

- The TISAX scheme was launched in 2017 and is managed by the ENX. (enx.com)

Brief introduction to TISAX: main goals

INDUSTRY

Creation of a common level of security for the automotive industry

QUALITY

Ensure the comparability and quality of the assessments

CHECK

Ensuring common recognition of the audit (VDA ISA)

RESULTS

Exchange best practices and experiences

COSTS

Reduce cost, effort and complexity

SHARE

The auditee can freely choose with whom and in what level of detail they share their results.

TISAX® requirements (IS, 45 controls)

Information security management

The company must have an information security management system (ISMS) in place that complies with the requirements of the international standard ISO/IEC 27001.

HR

The company must have a good control of its human resources and provide sufficient training to employees and stakeholders.

Physical security

The company must have measures in place to protect its physical assets, such as buildings, equipment, and documents, from unauthorized access, theft, and damage.

Business continuity

The company must have plans in place to ensure the continuity of its business operations in the event of a security incident or other disruption.

Incident management

The company must have procedures in place to detect, report, and respond to security incidents and breaches.

Access controls

The company must have controls in place to ensure that only authorized individuals have access to its information systems and data

Third-party management

The company must have processes in place to manage the security of its third-party suppliers and service providers.

Legal and Data protection

The company must have measures in place to protect personal data in accordance with GDPR and other applicable data protection laws.

TISAX® requirements (IS, 45 controls)

Information security management

The company must have an information security management system (ISMS) in place that complies with the requirements of the international standard ISO/IEC 27001.

HR

The company must have a good control of its human resources and provide sufficient training to employees and stakeholders.

Physical security

The company must have measures in place to protect its physical assets, such as buildings, equipment, and documents, from unauthorized access, theft, and damage.

Business continuity

The company must have plans in place to ensure the continuity of its business operations in the event of a security incident or other disruption.

Incident management

The company must have procedures in place to detect, report, and respond to security incidents and breaches.

Access controls

The company must have controls in place to ensure that only authorized individuals have access to its information systems and data

Third-party management

The company must have processes in place to manage the security of its third-party suppliers and service providers.

Legal and Data protection

The company must have measures in place to protect personal data in accordance with GDPR and other applicable data protection laws.

TISAX® requirements (PP, 22 controls)

Physical security

The customer must have controls in place for external/internal physical security of its facilities

Organizational Requirements

All customers handling prototypes or parts must have special controls in place for legal compliance, subcontracting, classification and photography.

Handling of vehicles

The customer must have a measure to protect vehicles, proto parts and components during transportation and parking.

Trial vehicles

The customer must have procedures in place to protect trial vehicles following customer-specific requirements.

Events and shootings

The company must have in place specific controls regarding planning, preparation or execution of events or shootings.

TISAX® requirements (DP, 12 controls)

Data Protection

The company must have a good data protection control to determine the basic suitability of a service provider to act as a processor within the meaning of Article 28 of the EU GDPR.

Main differentiation between TISAX and ISO27001.

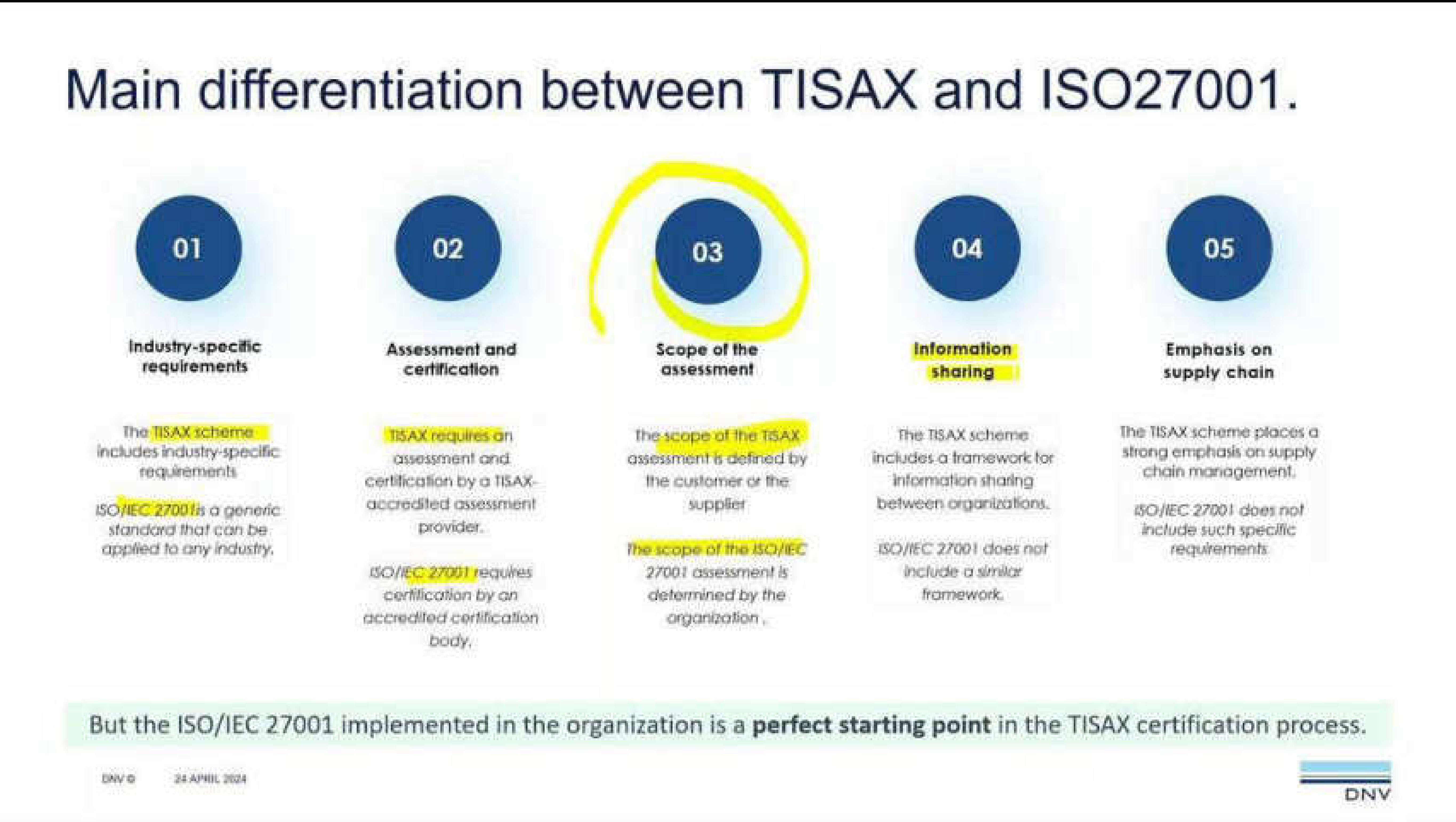
01

02

03

04

05



Main differentiation between TISAX and ISO27001.

01

Industry-specific requirements

The TISAX scheme includes industry-specific requirements.

ISO/IEC 27001is a generic standard that can be applied to any industry.

02

Assessment and certification

TISAX requires an assessment and certification by a TISAX-accredited assessment provider.

ISO/IEC 27001 requires certification by an accredited certification body.

03

Scope of the assessment

the scope of the TISAX assessment is defined by the customer or the supplier

The scope of the ISO/IEC 27001 assessment is determined by the organization .

04

Information sharing

The TISAX scheme includes a framework for information sharing between organizations.

ISO/IEC 27001 does not include a similar framework.

05

Emphasis on supply chain

The TISAX scheme places a strong emphasis on supply chain management.

ISO/IEC 27001 does not include such specific requirements.

But the ISO/IEC 27001 implemented in the organization is a **perfect starting point** in the TISAX certification process.

Is it difficult to implement TISAX if I have ISO27001?

If your organization already has an ISO 27001-certified Information Security Management System (ISMS), you are in a **good position to implement TISAX**.

- TISAX builds on ISO 27001 and includes **additional industry-specific requirements** that are specific to the automotive industry.

- To ensure a successful TISAX certification, it's important to fully understand the TISAX requirements and how they differ from ISO 27001.

- Working with an experienced ***TISAX consultant*** can also help ensure a smooth and successful TISAX certification process.

5 reasons why company should get TISAX ®

1. INDUSTRY STANDARDS

TISAX certification demonstrates a company's commitment to information security and its ability to meet the stringent requirements of the standard.

2. IMPROVED REPUTATION

TISAX certification can enhance a company's reputation and credibility.

3. COMPETITIVE ADVANTAGE

TISAX certification can provide a competitive advantage over companies that have not been certified.

4. INCREASED TRUST

TISAX certification can increase trust and confidence among stakeholders.

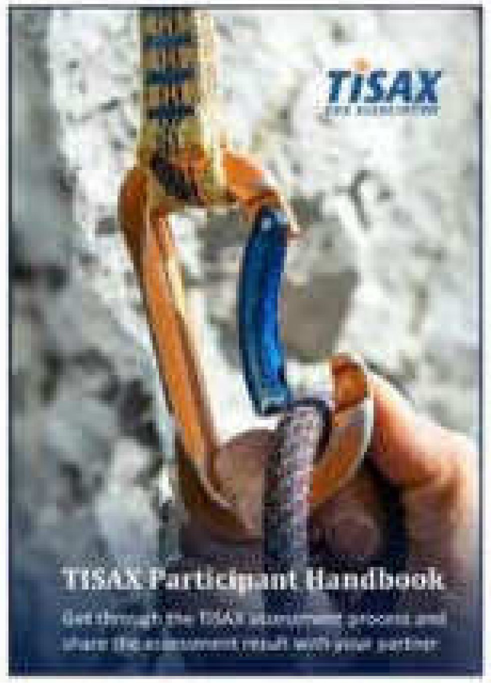
5. REDUCED RISK

TISAX certification can help reduce the risk of data breaches, cyber attacks, and other security incidents.

Documents

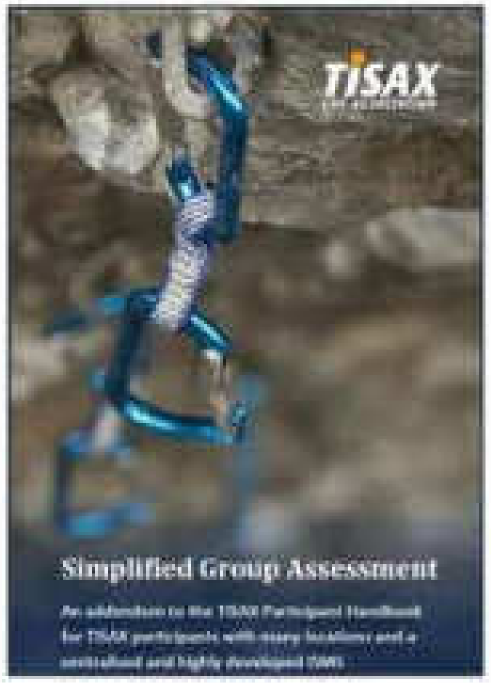
essentials for implementation, training and audits

Minimum documents/material: *enx.com*



TISAX Participant Handbook

Get through the TISAX assessment process and share the assessment result with your partner



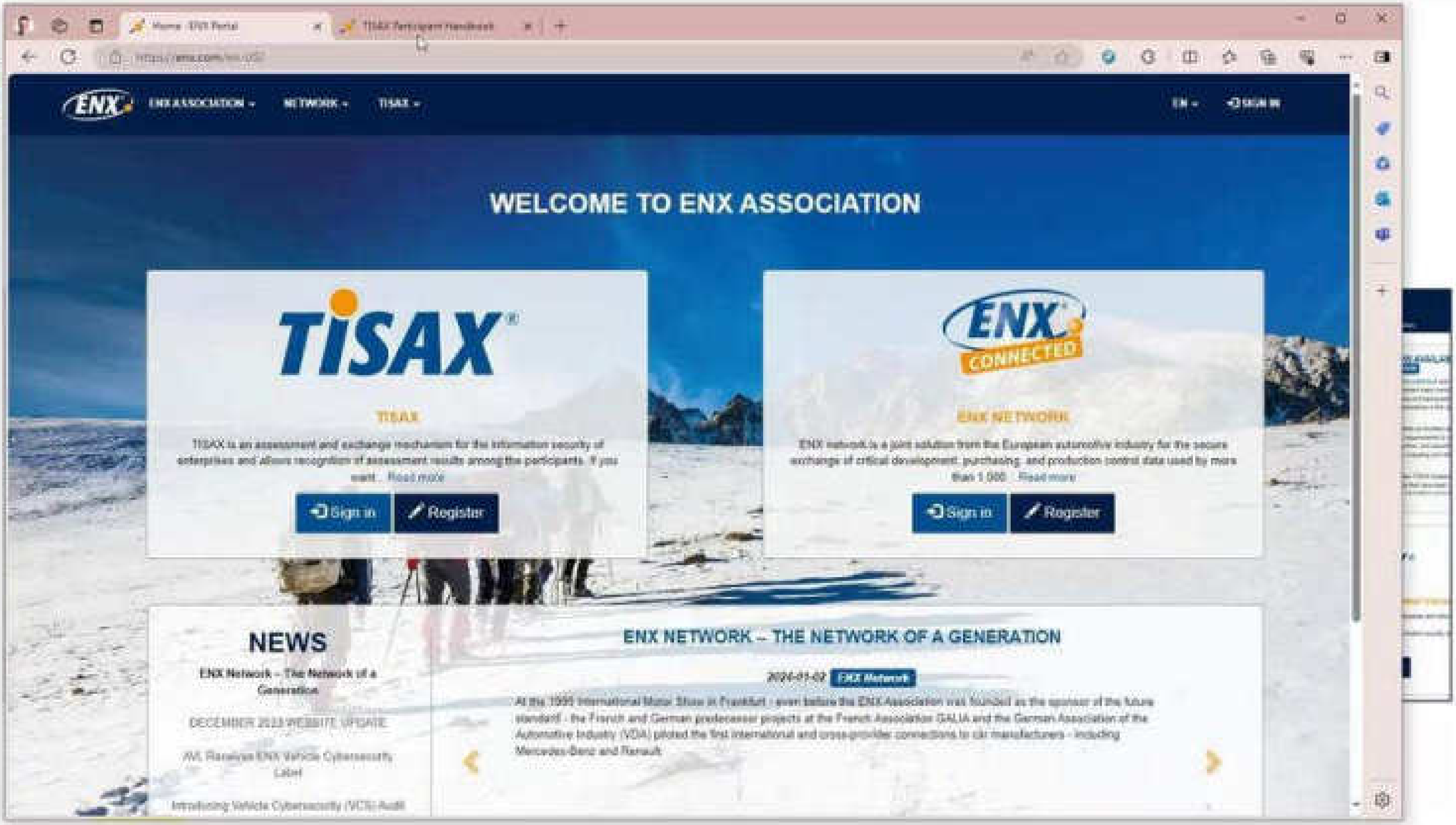
Simplified Group Assessment

An addendum to the TISAX Participant Handbook for TISAX participants with many locations and a centralised and highly developed ISMS

TISAX NEWS

ISA VERSION 6 NOW AVAILA

M



WELCOME TO ENX ASSOCIATION

TISAX

TISAX is an assessment and exchange mechanism for the information security of enterprises and allows recognition of assessment results among the participants. If you want... Read more

ENX NETWORK

ENX network is a joint solution from the European automotive industry for the secure exchange of critical development, purchasing, and production control data used by more than 1,000... Read more

NEWS

ENX Network – The Network of a Generation

DECEMBER 2023 WEBSITE UPDATE

AVL Receives ENX Vehicle Cybersecurity Label

Introducing Vehicle Cybersecurity (VCS) Audit

ENX NETWORK – THE NETWORK OF A GENERATION

2024-01-02 ENX Network

At the 1995 International Motor Show in Frankfurt - even before the ENX Association was founded as the sponsor of the future standard! - the French and German predecessor projects at the French Association GALIA and the German Association of the Automotive Industry (VDA) piloted the first international and cross-provider connections to car manufacturers - including Mercedes-Benz and Renault.

M

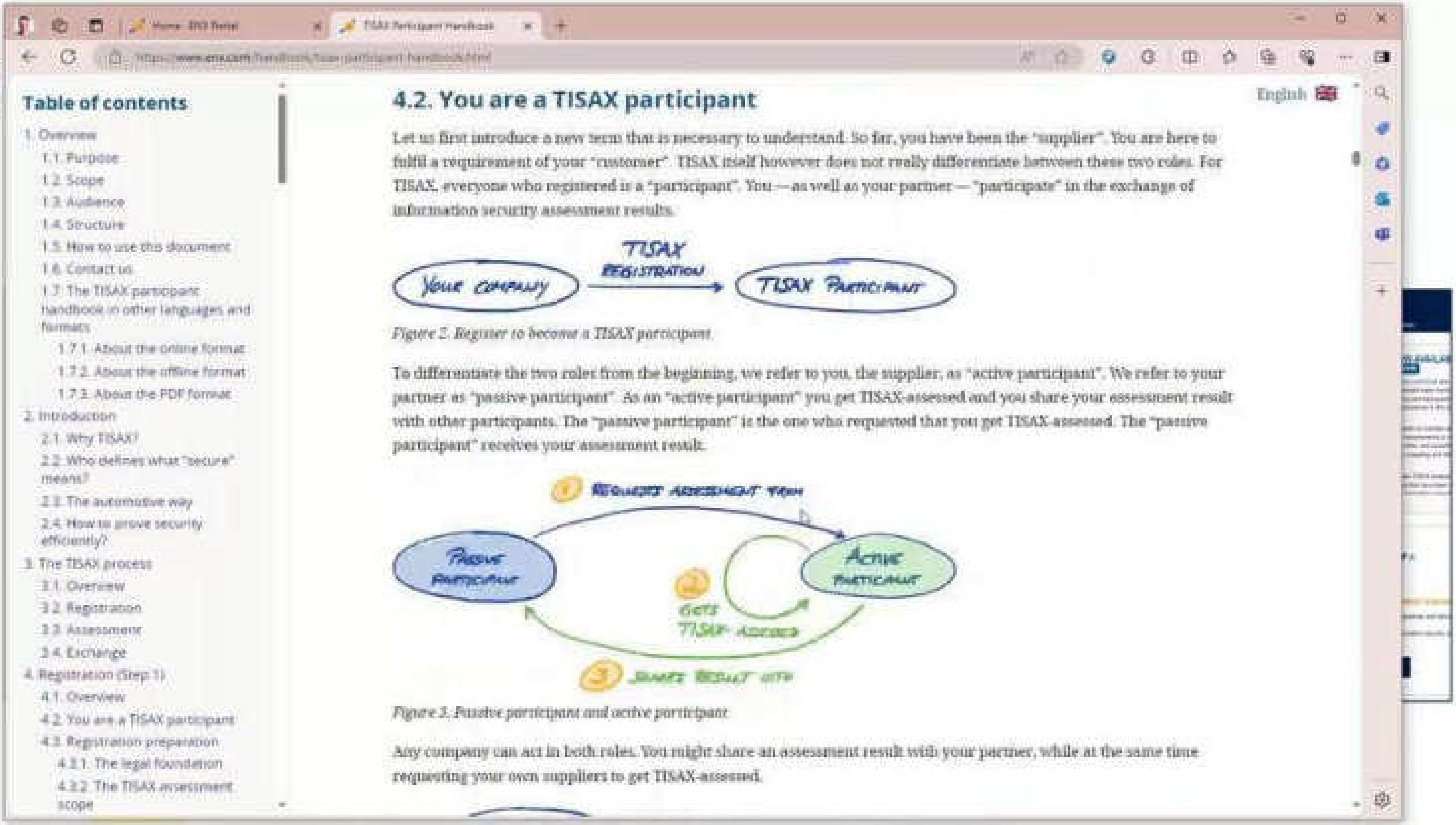

Home - ENX Portal
TISAX Participant Handbook
https://www.enx.com/handbook/tisax-participant-handbook.html
English

Table of contents

4.2. You are a TISAX participant

Let us first introduce a new term that is necessary to understand. So far, you have been the "supplier". You are here to fulfil a requirement of your "customer". TISAX itself however does not really differentiate between these two roles. For TISAX, everyone who registered is a "participant". You — as well as your partner — "participate" in the exchange of information security assessment results.

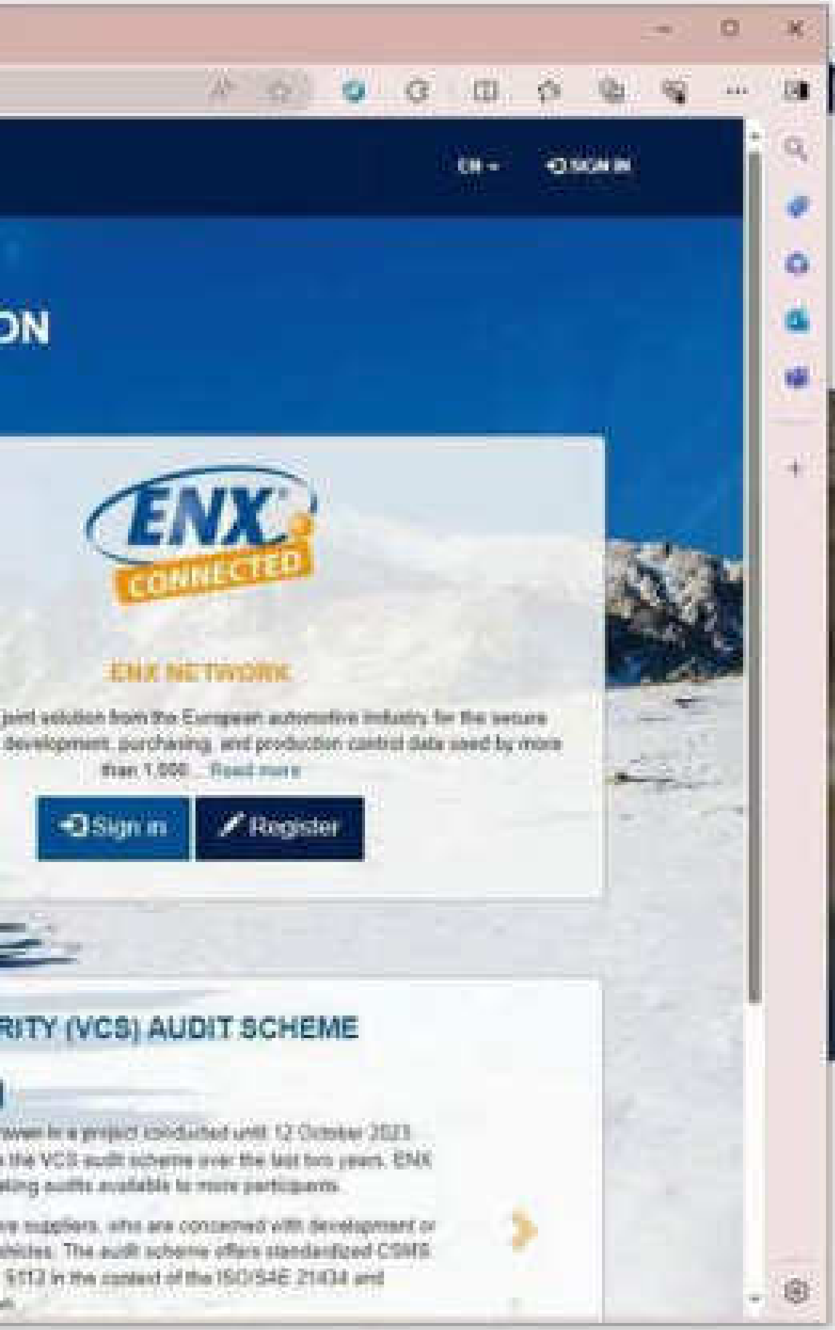
Figure 2. Register to become a TISAX participant

To differentiate the two roles from the beginning, we refer to you, the supplier, as "active participant". We refer to your partner as "passive participant". As an "active participant" you get TISAX-assessed and you share your assessment result with other participants. The "passive participant" is the one who requested that you get TISAX-assessed. The "passive participant" receives your assessment result.

Figure 3. Passive participant and active participant

Any company can act in both roles. You might share an assessment result with your partner, while at the same time requesting your own suppliers to get TISAX-assessed.

nents/material: *enx.com*



ON

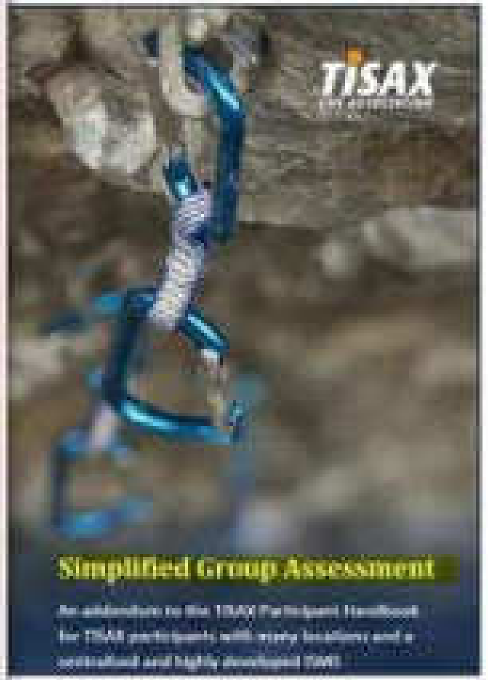
ENX NETWORK

joint solution from the European automotive industry for the secure development, purchasing, and production control data used by more than 1,000 ... Read more

RITY (VCS) AUDIT SCHEME

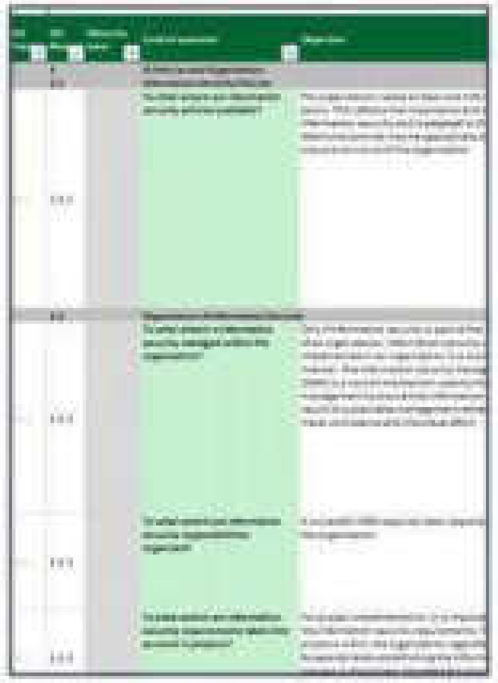
tween in a project conducted until 12 October 2023 the VCS audit scheme over the last two years. ENX ating audits available to more participants.

re suppliers, who are concerned with development or vehicles. The audit scheme offers standardized CSMS 5112 in the context of the ISO/SAE 21434 and



Simplified Group Assessment

An addendum to the TISAX Participant Handbook for TISAX participants with many locations and a centralised and highly developed ISMS



2

TISAX
TISAX Participant handbook

TISAX
TISAX Teilnehmerhandbuch

TISAX
Manuel du participant TISAX

TISAX

TISAX
Manual del participante de TISAX

TISAX

TISAX
Manual do participante do TISAX

TISAX
Manuale partecipanti TISAX

TISAX
TISAX 참가자 안내서

TISAX
Příručka pro účastníky v TISAX

TISAX
Podręcznik uczestnika TISAX

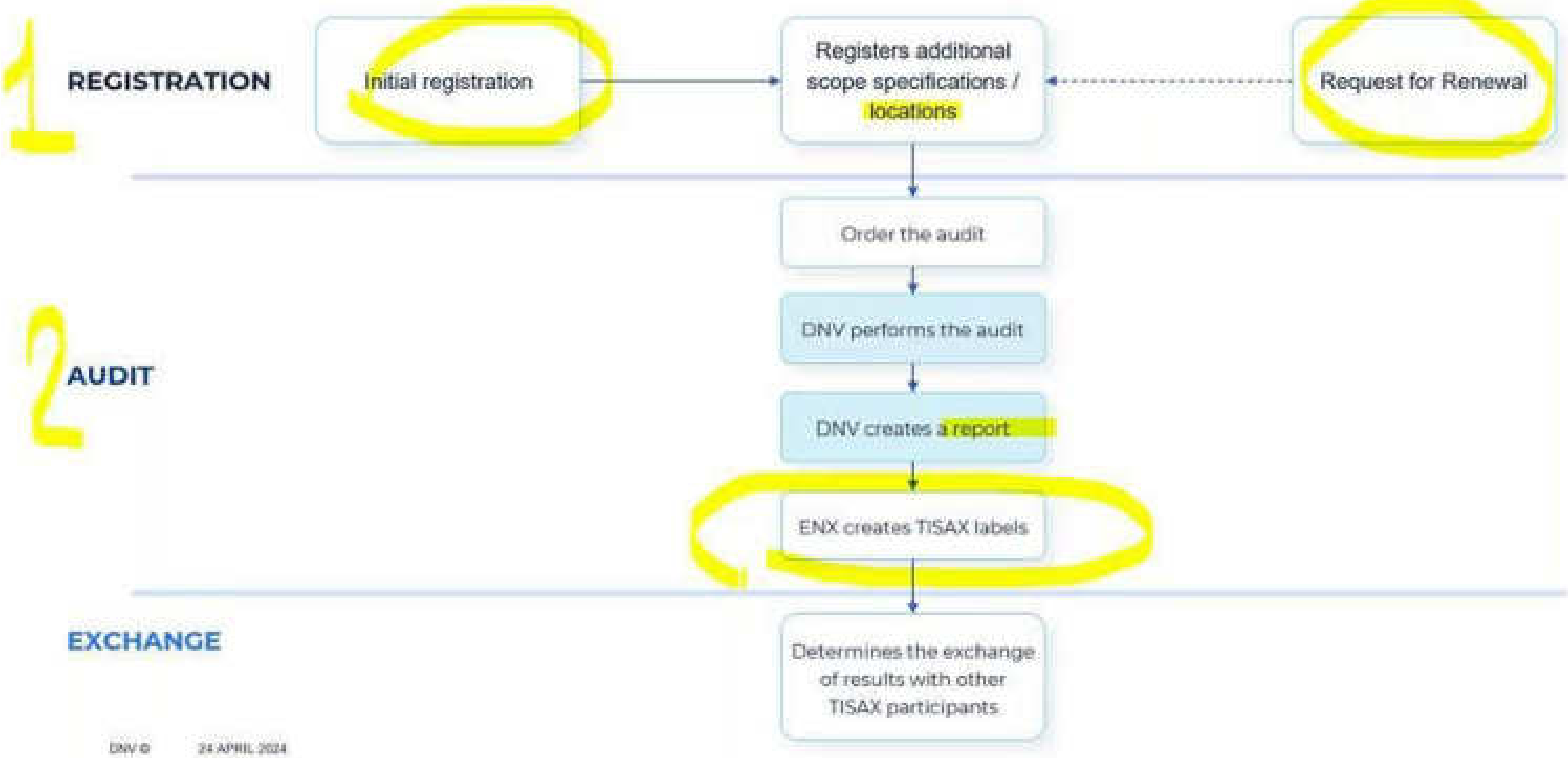
TISAX certification process

label lifecycle

Overview TISAX process

EXCHANGE

Overview TISAX process



1

REGISTRATION

Initial registration

Registers additional scope specifications / locations

Request for Renewal

2

AUDIT

Order the audit

DNV performs the audit

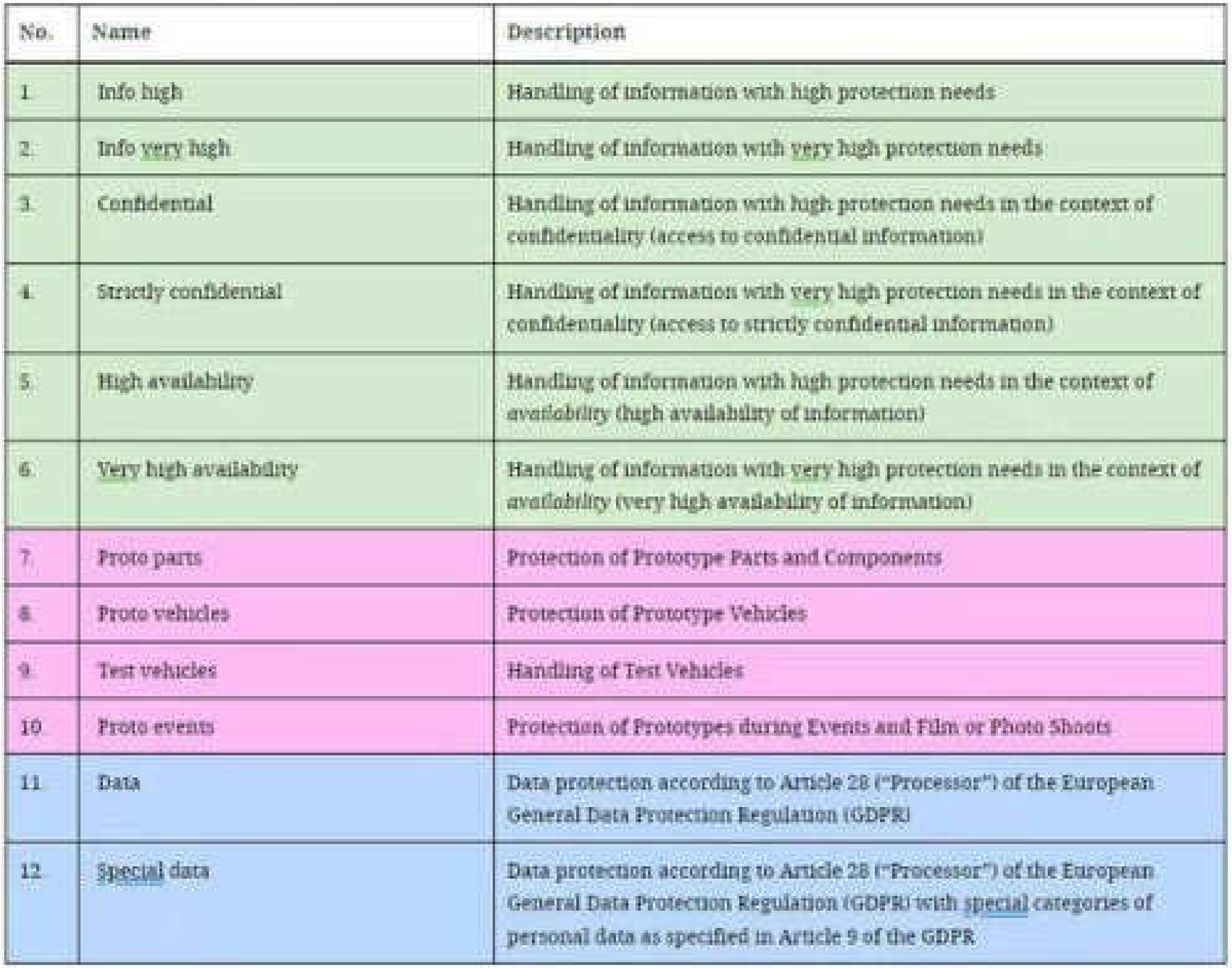
DNV creates a report

ENX creates TISAX labels

EXCHANGE

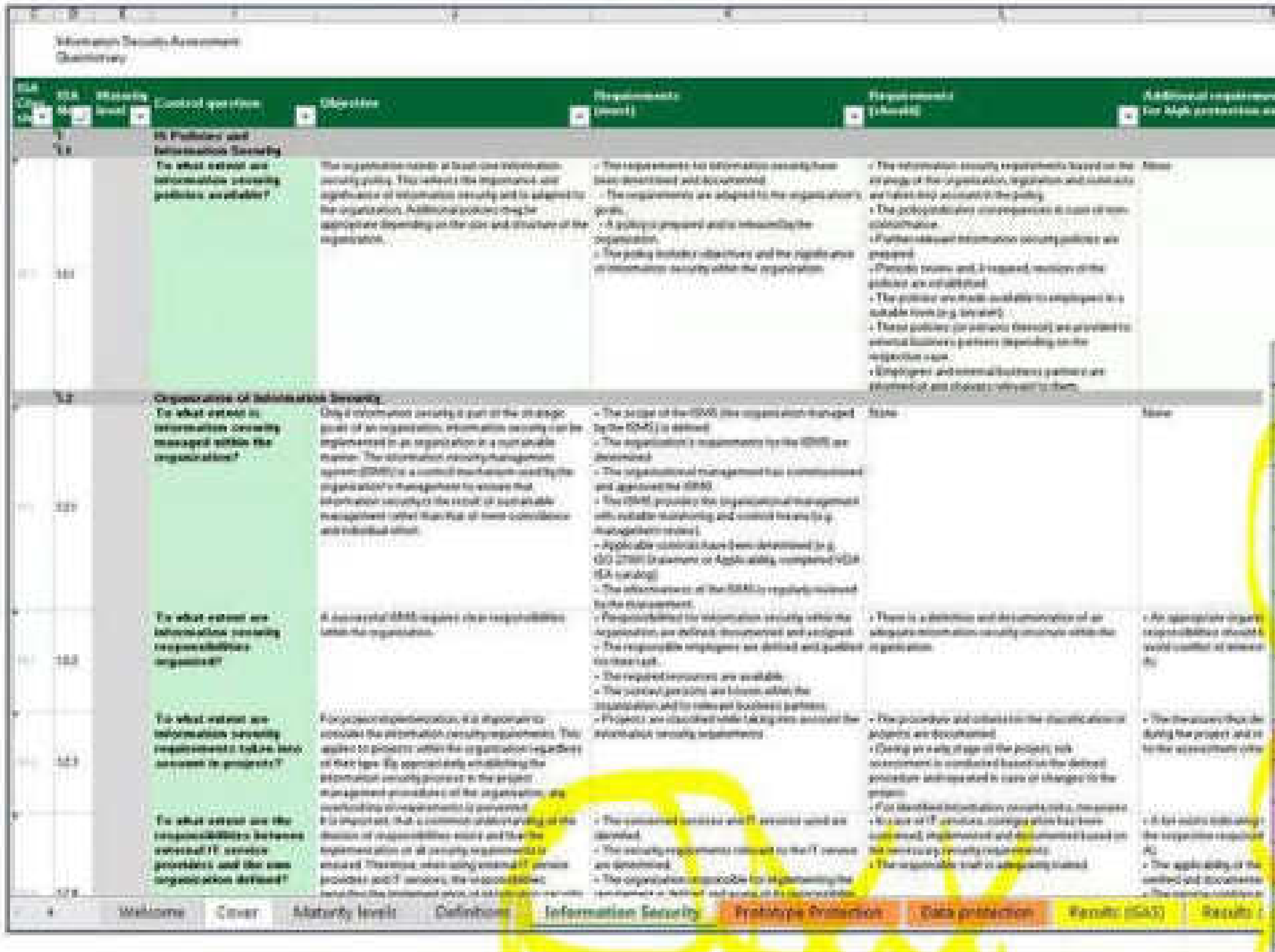
Determines the exchange of results with other TISAX participants

Assessment objectives



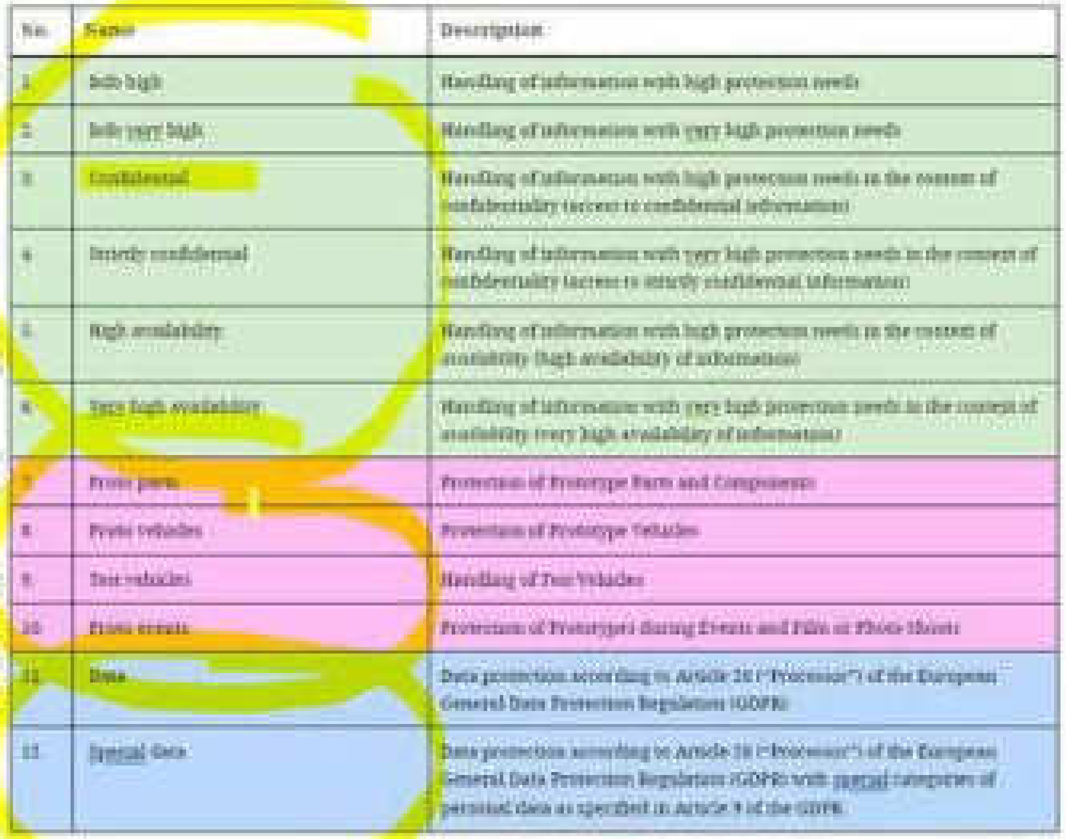
	No.	Name	Description	
INFO SEC	1.	Info high	Handling of information with high protection needs	AL2
	2.	Info very high	Handling of information with very high protection needs	AL3
	3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information)	AL2
	4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information)	AL3
	5.	High availability	Handling of information with high protection needs in the context of availability (high availability of information)	AL2
	6.	Very high availability	Handling of information with very high protection needs in the context of availability (very high availability of information)	AL3
PROTO	7.	Proto parts	Protection of Prototype Parts and Components	AL3
	8.	Proto vehicles	Protection of Prototype Vehicles	AL3
	9.	Test vehicles	Handling of Test Vehicles	AL3
	10	Proto events	Protection of Prototypes during Events and Film or Photo Shoots	AL3
DATA	11	Data	Data protection according to Article 28 ("Processor") of the European General Data Protection Regulation (GDPR)	AL2
	12	Special data	Data protection according to Article 28 ("Processor") of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR	AL3

Assessment objectives



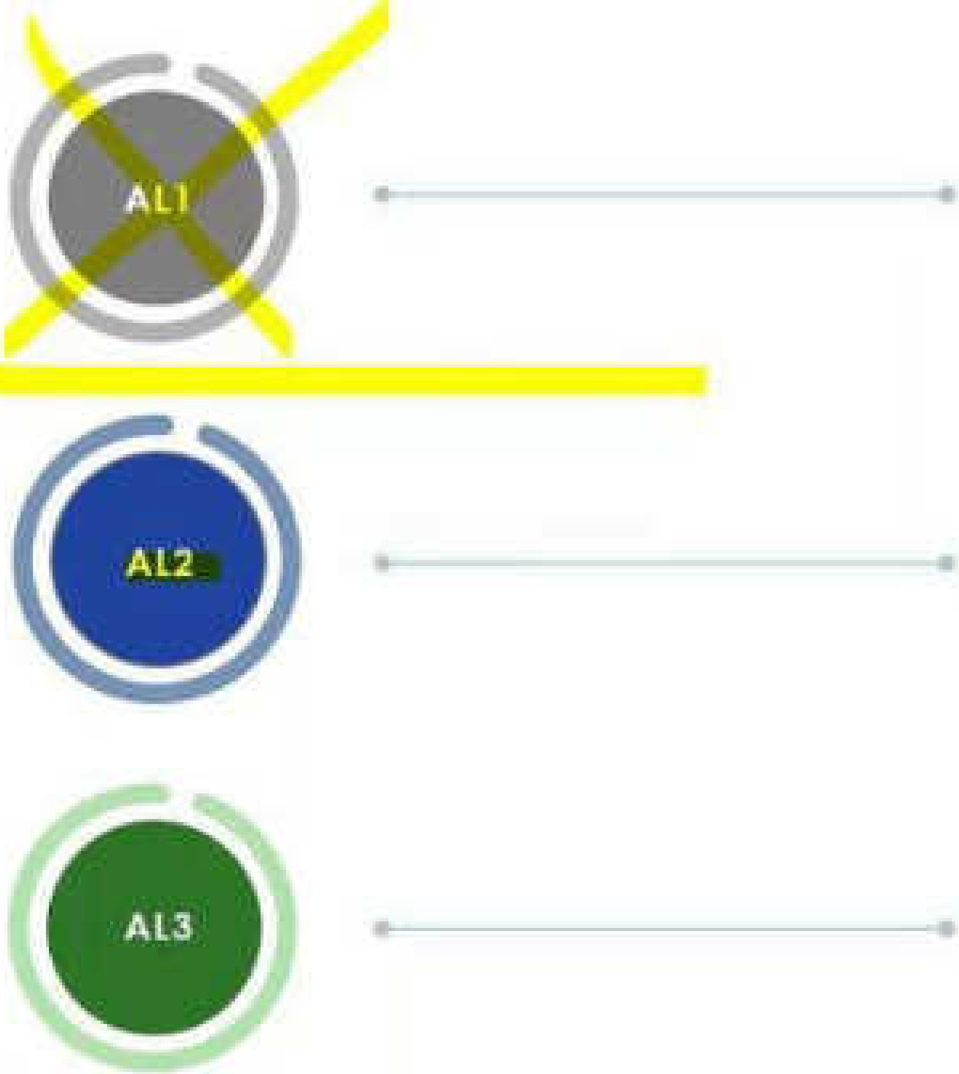
Information Security Assessment
Questionnaire

ISA Chap…	ISA No.	Maturity level	Control question	Objective	Requirements (must)	Requirements (should)	Additional requirements for high protection needs	Additio… for very…
	1 1.1		IS Policies and Information Security					
	1.1.1		To what extent are information security policies available?	The organization needs at least one information security policy. This reflects the importance and significance of information security and is adapted to the organization. Additional policies may be appropriate depending on the size and structure of the organization.	- The requirements for information security have been determined and documented: - The requirements are adapted to the organization's goals. - A policy is prepared and is released by the organization. - The policy includes objectives and the significance of information security within the organization.	- The information security requirements based on the strategy of the organization, legislation and contracts are taken into account in the policy. - The policy indicates consequences in case of non-compliance. - Further relevant information security policies are prepared. - Periodic review and, if required, revision of the policies are established. - The policies are made available to employees in a suitable form (e.g. intranet). - These policies (or extracts thereof) are provided to external business partners depending on the respective case. - Employees and external business partners are informed of and changes relevant to them.	None	None
	1.2		Organization of Information Security					
	1.2.1		To what extent is information security managed within the organization?	Only if information security is part of the strategic goals of an organization, information security can be implemented in an organization in a sustainable manner. The information security management system (ISMS) is a control mechanism used by the organization's management to ensure that information security is the result of sustainable management rather than that of mere coincidence and individual effort.	- The scope of the ISMS (the organization managed by the ISMS) is defined. - The organization's requirements for the ISMS are determined. - The organizational management has commissioned and approved the ISMS. - The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). - Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed VDA ISA catalog). - The effectiveness of the ISMS is regularly reviewed by the management.	None	None	
	1.2.2		To what extent are information security responsibilities organized?	A successful ISMS requires clear responsibilities within the organization.	- Responsibilities for information security within the organization are defined, documented and assigned. - The responsible employees are defined and qualified for their task. - The required resources are available. - The contact persons are known within the organization and to relevant business partners.	- There is a definition and documentation of an adequate information security structure within the organization.	- An appropriate organiz… responsibilities should b… avoid conflict of interest… ds.	
	1.2.3		To what extent are information security requirements taken into account in projects?	For project implementation, it is important to consider the information security requirements. This applies to projects within the organization regardless of their type. By appropriately establishing the information security process in the project management procedures of the organization, the overlooking of requirements is prevented.	- Projects are classified while taking into account the information security requirements.	- The procedure and criteria for the classification of projects are documented. - During an early stage of the project, risk assessment is conducted based on the defined procedure and repeated in case of changes to the project. - For identified information security risks, measures	- The measures thus de… during the project and… to the assessment crite…	
	1.2.4		To what extent are the responsibilities between external IT service providers and the own organization defined?	It is important, that a common understanding of the division of responsibilities exists and that the implementation of all security requirements is ensured. Therefore, when using external IT service providers and IT services, the responsibilities regarding the implementation of information security	- The concerned services and IT services used are identified. - The security requirements relevant to the IT service are determined. - The organization responsible for implementing the requirement is defined and aware of its responsibility	- In case of IT services, configuration has been reviewed, implemented and documented based on the necessary security requirements. - The responsible staff is adequately trained.	- A list exists indicating… the respective responsib… (e.g. … - The applicability of the… verified and documente…	



No.	Name	Description
1	Info high	Handling of information with high protection needs
2	Info very high	Handling of information with very high protection needs
3	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information)
4	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information)
5	High availability	Handling of information with high protection needs in the context of availability (high availability of information)
6	Very high availability	Handling of information with very high protection needs in the context of availability (very high availability of information)
7	Proto parts	Protection of Prototype Parts and Components
8	Proto vehicles	Protection of Prototype Vehicles
9	Test vehicles	Handling of Test Vehicles
10	Proto events	Protection of Prototypes during Events and Film or Photo Shoots
11	Data	Data protection according to Article 28 ("Processor") of the European General Data Protection Regulation (GDPR)
12	Special data	Data protection according to Article 28 ("Processor") of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR

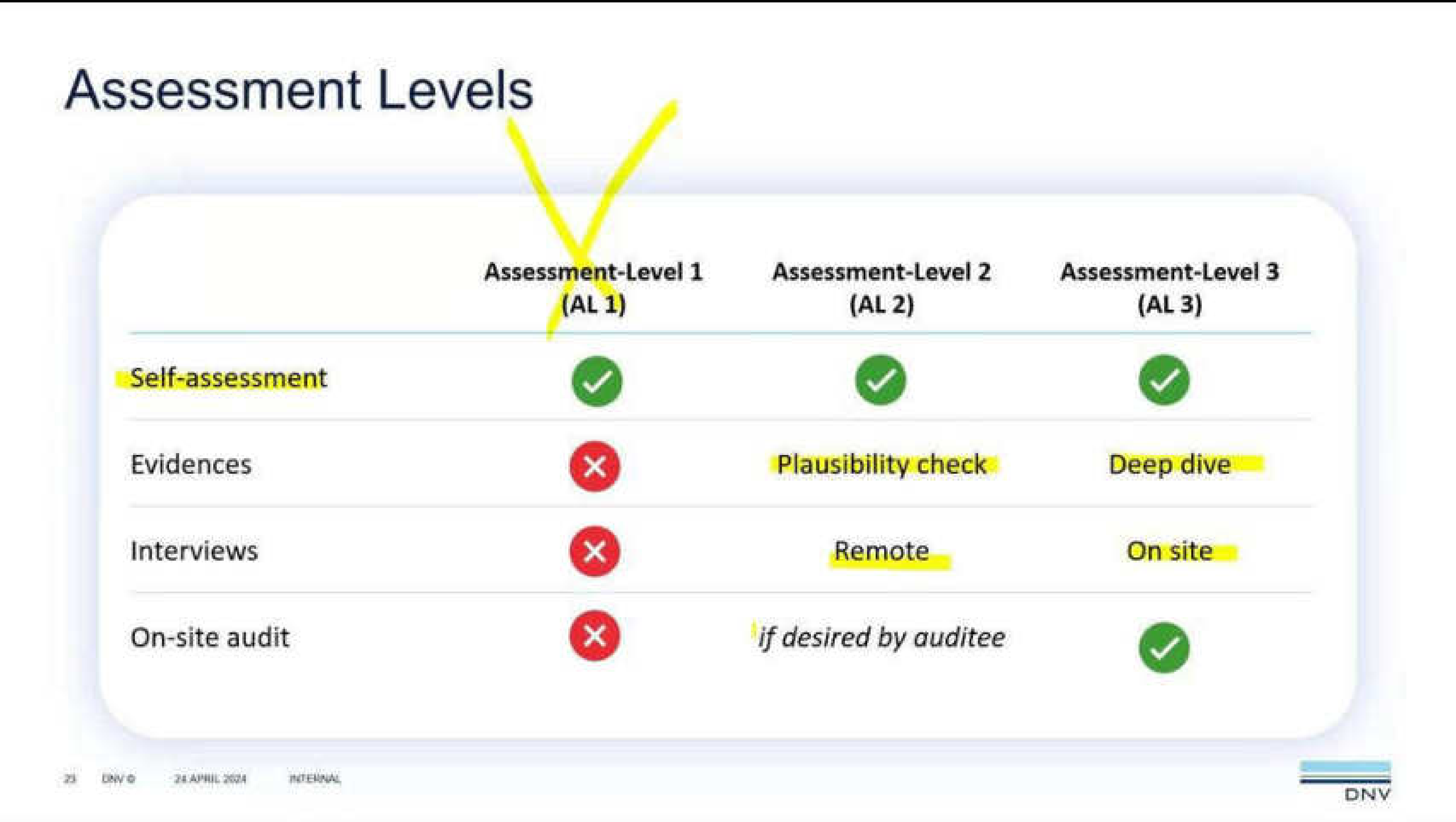
AL: Assessment Levels



Assessments in assessment level 1 are mainly for internal purposes in the true sense of a **self-assessment**.

For an assessment in assessment level 2, the audit provider does a plausibility check on customer' self-assessment. The audit provider does the interview generally **on-line**.

For an assessment in assessment level 3, the audit provider does a comprehensive verification of your company's compliance with the applicable requirements. **Onsite** audit & Interviews.

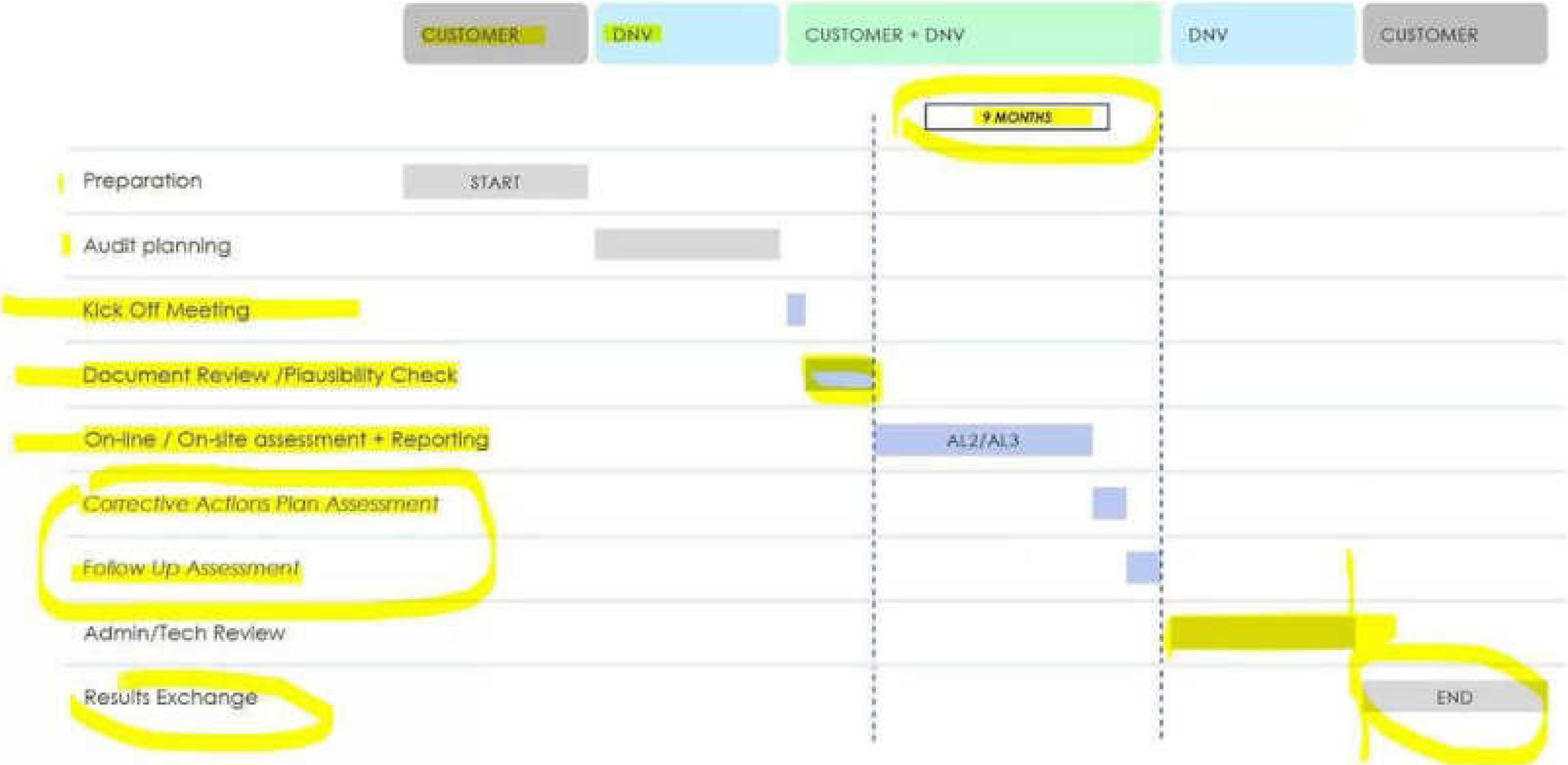


Assessment Levels

	Assessment-Level 1 (AL 1)	Assessment-Level 2 (AL 2)	Assessment-Level 3 (AL 3)
Self-assessment	✓	✓	✓
Evidences	✗	Plausibility check	Deep dive
Interviews	✗	Remote	On site
On-site audit	✗	*if desired by auditee*	✓

TISAX® audit

standardized process



CUSTOMER | DNV | CUSTOMER + DNV | DNV | CUSTOMER

9 MONTHS

Preparation — START

Audit planning

Kick Off Meeting

Document Review /Plausibility Check

On-line / On-site assessment + Reporting — AL2/AL3

Corrective Actions Plan Assessment

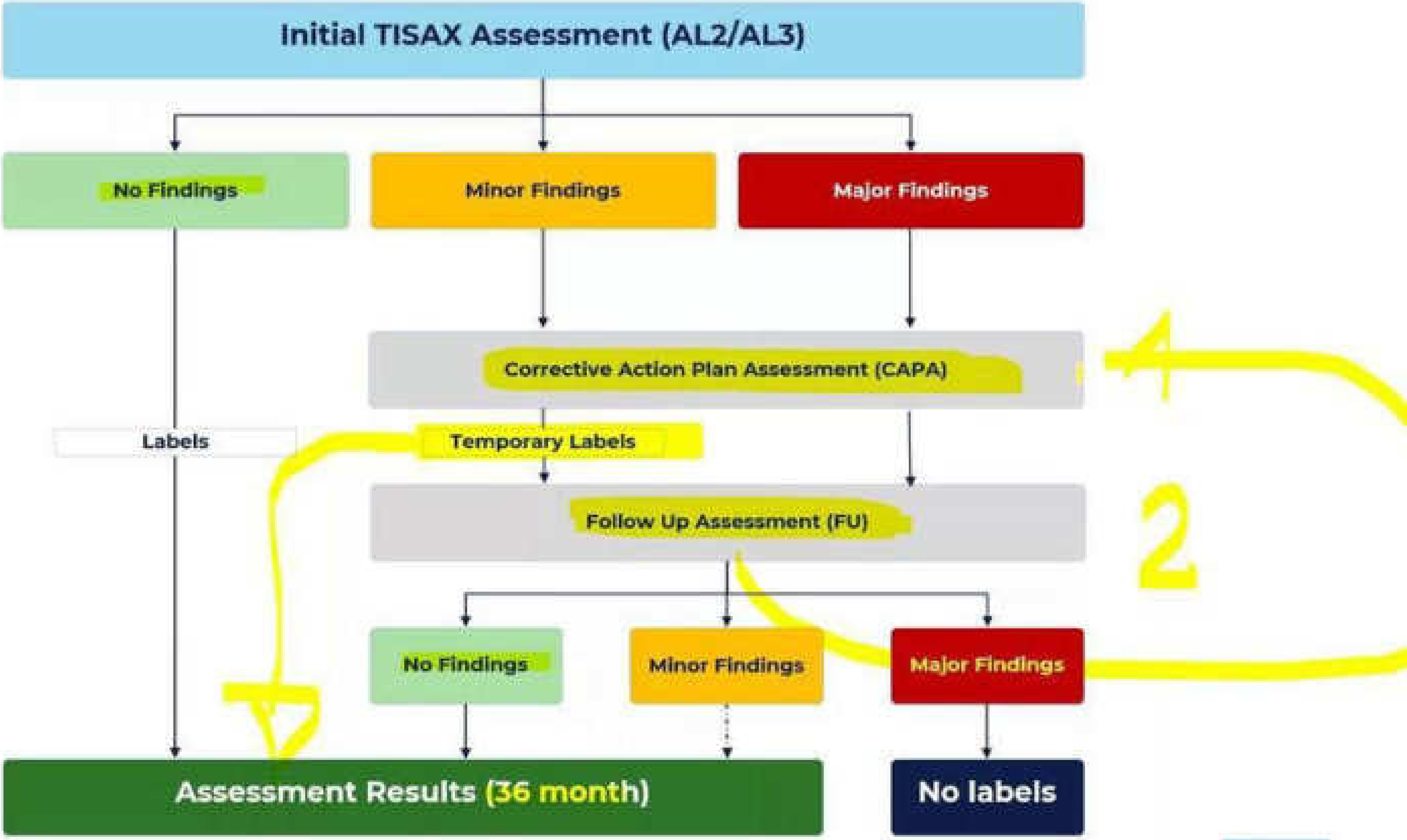
Follow Up Assessment

Admin/Tech Review

Results Exchange — END

DNV Audit Overview

Kick Off Meeting	Document Review	Audit	Reporting
Online meeting	**Offline** Docs	**Online/Onsite** interviews	**Offline**
Following ENX rules (must be)	Evidences	Review all ISMS docs & guidelines	2 reports (preliminary/final)
No preparation by customer	Company website	Investigation	
		Onsite inspections (AL3)	



Initial TISAX Assessment (AL2/AL3)

No Findings

Minor Findings

Major Findings

Corrective Action Plan Assessment (CAPA)

Labels

Temporary Labels

Follow Up Assessment (FU)

No Findings

Minor Findings

Major Findings

Assessment Results (36 month)

No labels

VDA questionnaire

what to fill in? what to check?

DNV

TISAX®: web official + VDA ISA

Further recommendations: Handling the VDA catalogue

Fill in your relevant information according to the screenshot.

Maturity level:

Enter your maturity level here

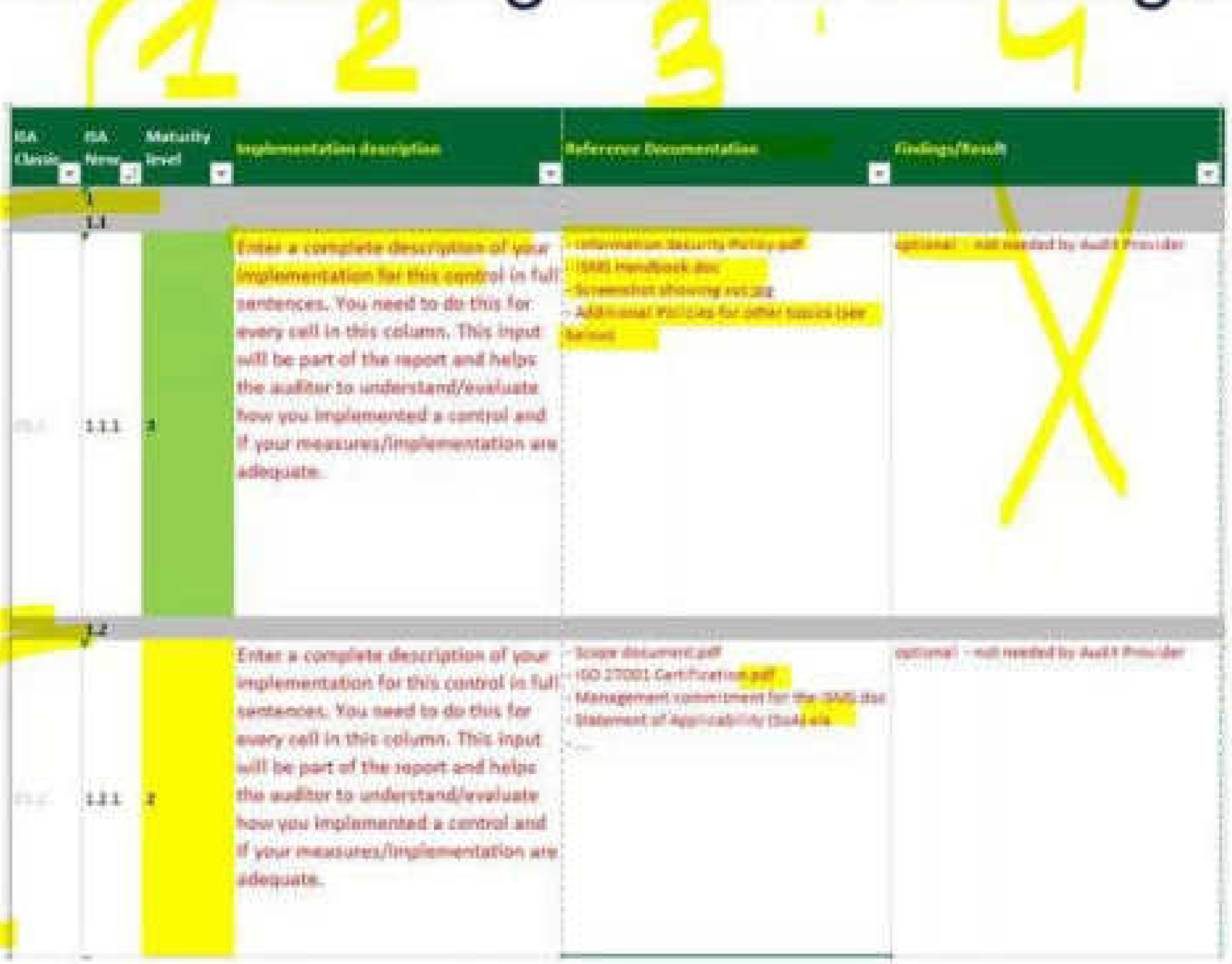
(the target is always "3").

Implementation description:

It is essential to have a full description of your implementation. Enter your description in full sentences.

Reference Documentation:

As part of the corresponding control, please enter the full file names of your evidences.

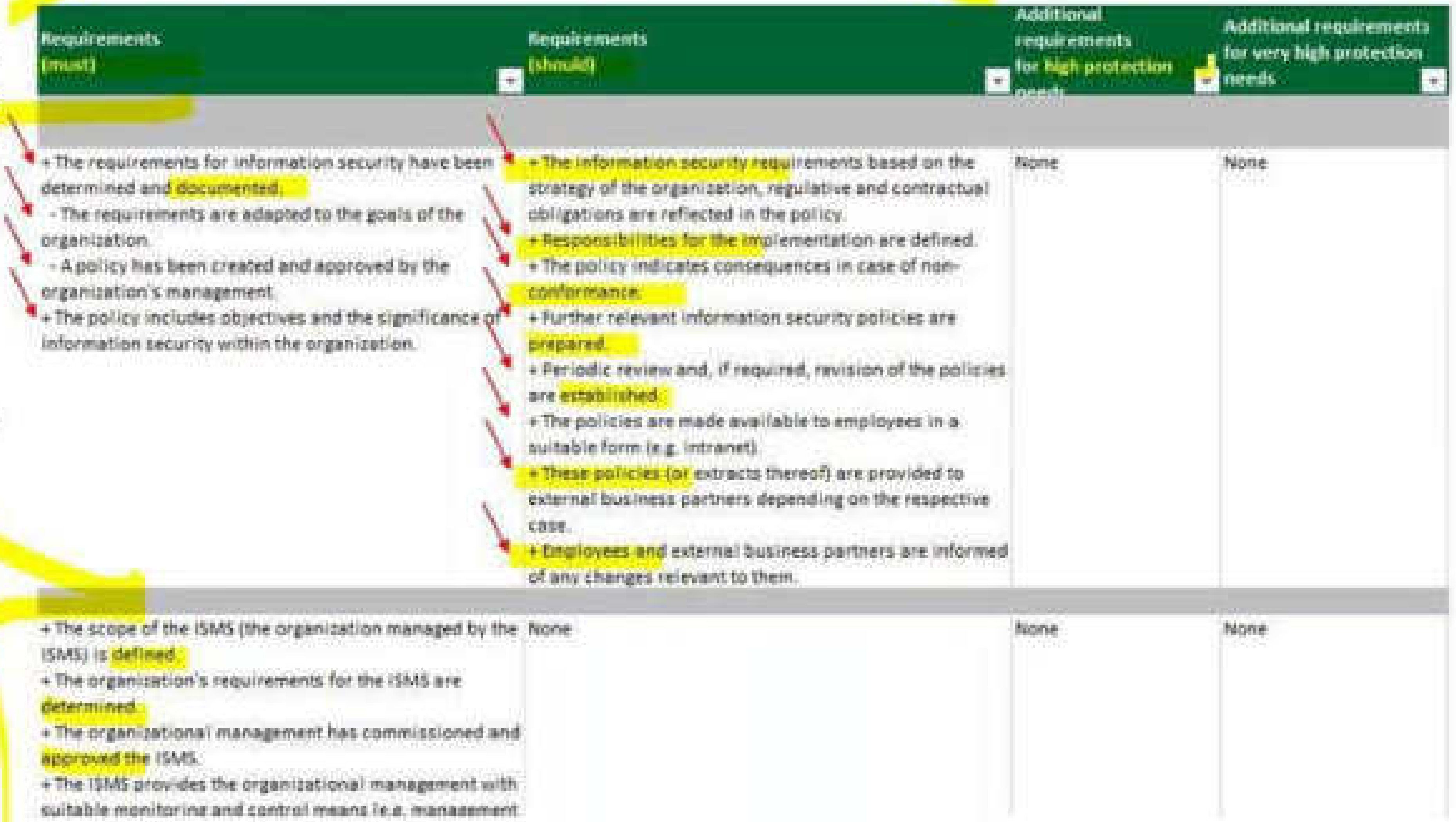


ISA Classic	ISA New	Maturity level	Implementation description	Reference Documentation	Findings/Result
	1				
	1.1				
[illegible]	1.1.1	3	Enter a complete description of your implementation for this control in full sentences. You need to do this for every cell in this column. This input will be part of the report and helps the auditor to understand/evaluate how you implemented a control and if your measures/implementation are adequate.	- Information Security Policy.pdf - ISMS Handbook.doc - Screenshot showing xxx.jpg - Additional Policies for other topics (see below)	optional - not needed by Audit Provider
	1.2				
[illegible]	1.2.1	2	Enter a complete description of your implementation for this control in full sentences. You need to do this for every cell in this column. This input will be part of the report and helps the auditor to understand/evaluate how you implemented a control and if your measures/implementation are adequate.	- Scope document.pdf - ISO 27001 Certification.pdf - Management commitment for the ISMS.doc - Statement of Applicability (SoA).xls - ...	optional - not needed by Audit Provider

Further recommendations: Handling the VDA catalogue

As part of the audit, you must be able to prove that you have implemented a measure / solution for each individual requirement.

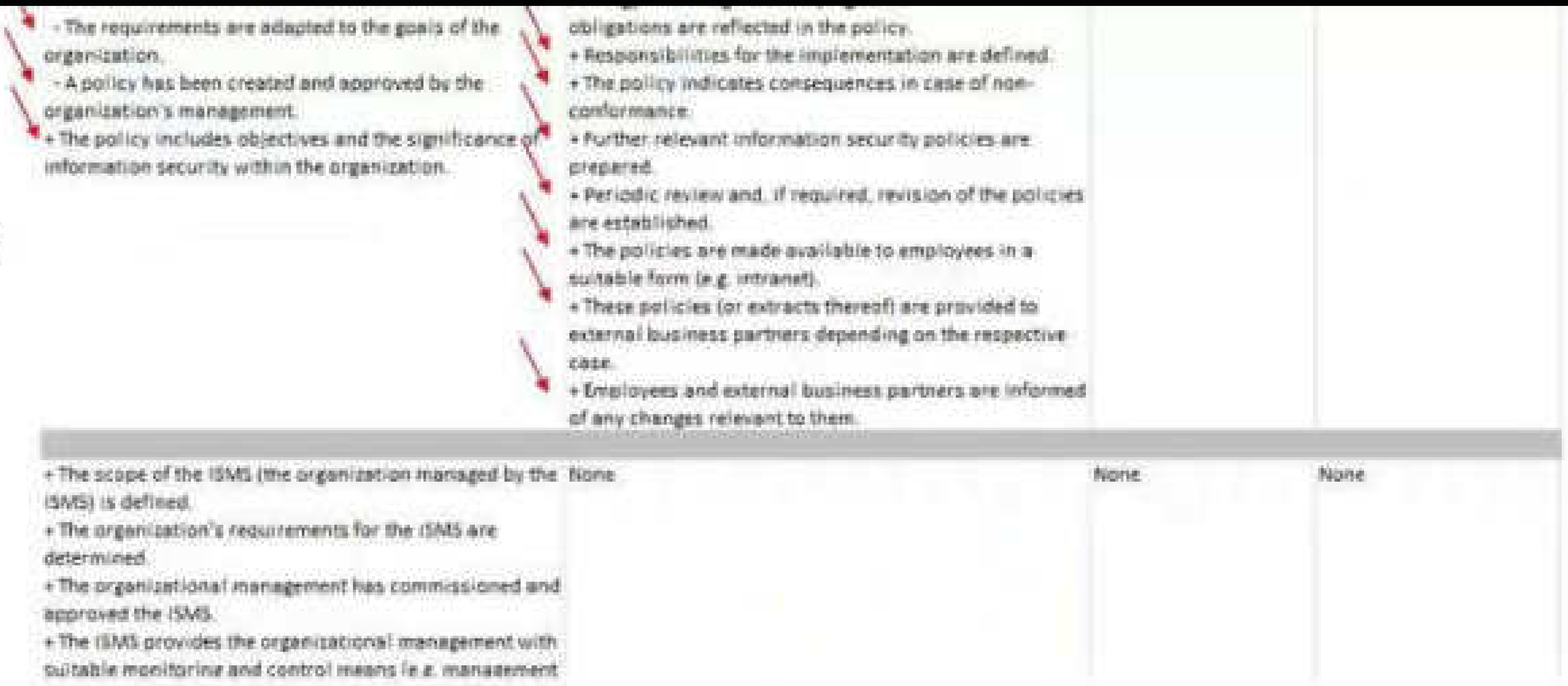
- "Must" requirements must be implemented.
- "Should" requirements must also be implemented (although you can explain why a particular requirement does not apply to you).
- "High" and "very high" requirements must be implemented (depending on your exam level)



Requirements (must)	Requirements (should)	Additional requirements for high protection needs	Additional requirements for very high protection needs
+ The requirements for information security have been determined and documented. - The requirements are adapted to the goals of the organization. - A policy has been created and approved by the organization's management. + The policy includes objectives and the significance of information security within the organization.	+ The information security requirements based on the strategy of the organization, regulative and contractual obligations are reflected in the policy. + Responsibilities for the implementation are defined. + The policy indicates consequences in case of non-conformance. + Further relevant information security policies are prepared. + Periodic review and, if required, revision of the policies are established. + The policies are made available to employees in a suitable form (e.g. intranet). + These policies (or extracts thereof) are provided to external business partners depending on the respective case. + Employees and external business partners are informed of any changes relevant to them.	None	None
+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management	None	None	None

requirement:

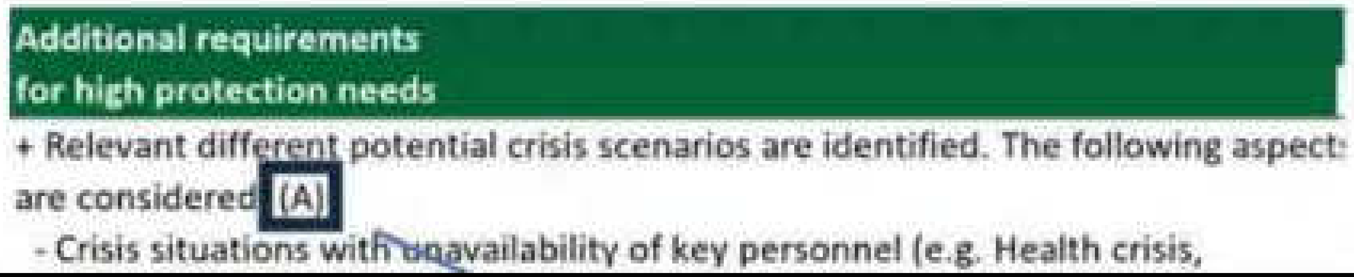
- "Must" requirements must be implemented.
- "Should" requirements must also be implemented (although you can explain why a particular requirement does not apply to you).
- "High" and "very high" requirements must be implemented (depending on your exam level)



- The requirements are adapted to the goals of the organization. - A policy has been created and approved by the organization's management. + The policy includes objectives and the significance of information security within the organization.	obligations are reflected in the policy. + Responsibilities for the implementation are defined. + The policy indicates consequences in case of non-conformance. + Further relevant information security policies are prepared. + Periodic review and, if required, revision of the policies are established. + The policies are made available to employees in a suitable form (e.g. intranet). + These policies (or extracts thereof) are provided to external business partners depending on the respective case. + Employees and external business partners are informed of any changes relevant to them.		
+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management	None	None	None

"C" apply for confidentiality labels

The new confidentiality labels follow the same logic as the availability labels and cover a subset of the requirements of the old "Info" labels.



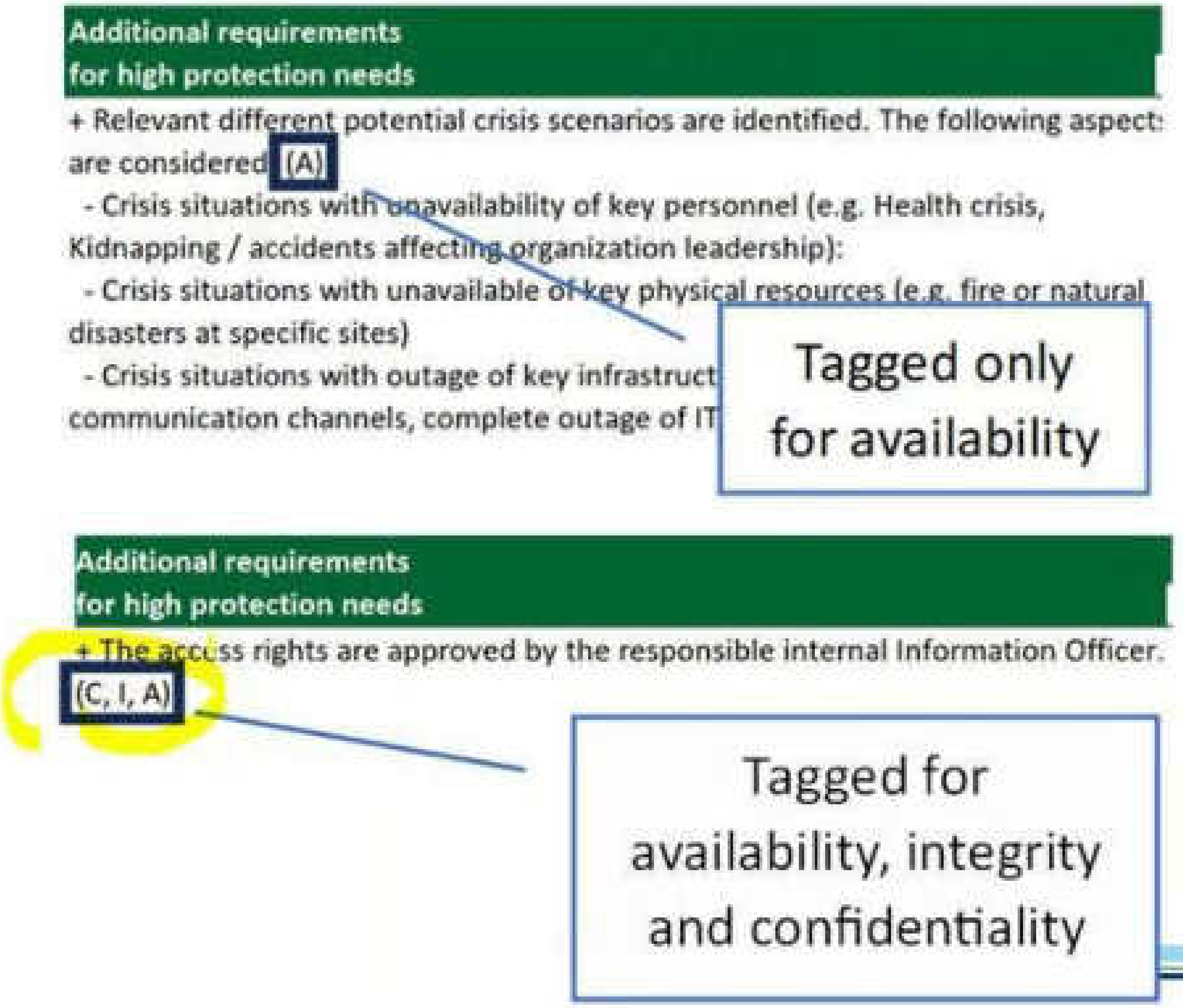
Additional requirements for high protection needs
+ Relevant different potential crisis scenarios are identified. The following aspect: are considered: [A] - Crisis situations with unavailability of key personnel (e.g. Health crisis,

“C” apply for confidentiality labels

The new confidentiality labels follow the same logic as the availability labels and cover a subset of the requirements of the old “Info” labels.

As the “Info” and availability labels, the confidentiality labels do refer to the “Information Security” tab of ISA and include all baseline requirements (“must” and “should”).

Since the tag does not contain a C these requirements are not applicable for confidentiality. This means, if you only select “Confidential” TISAX Assessment Objective, the auditor will not document any non-conformities regarding those requirements.



Additional requirements
for high protection needs

+ Relevant different potential crisis scenarios are identified. The following aspect: are considered: (A)
  - Crisis situations with unavailability of key personnel (e.g. Health crisis, Kidnapping / accidents affecting organization leadership):
  - Crisis situations with unavailable of key physical resources (e.g. fire or natural disasters at specific sites)
  - Crisis situations with outage of key infrastruct communication channels, complete outage of IT

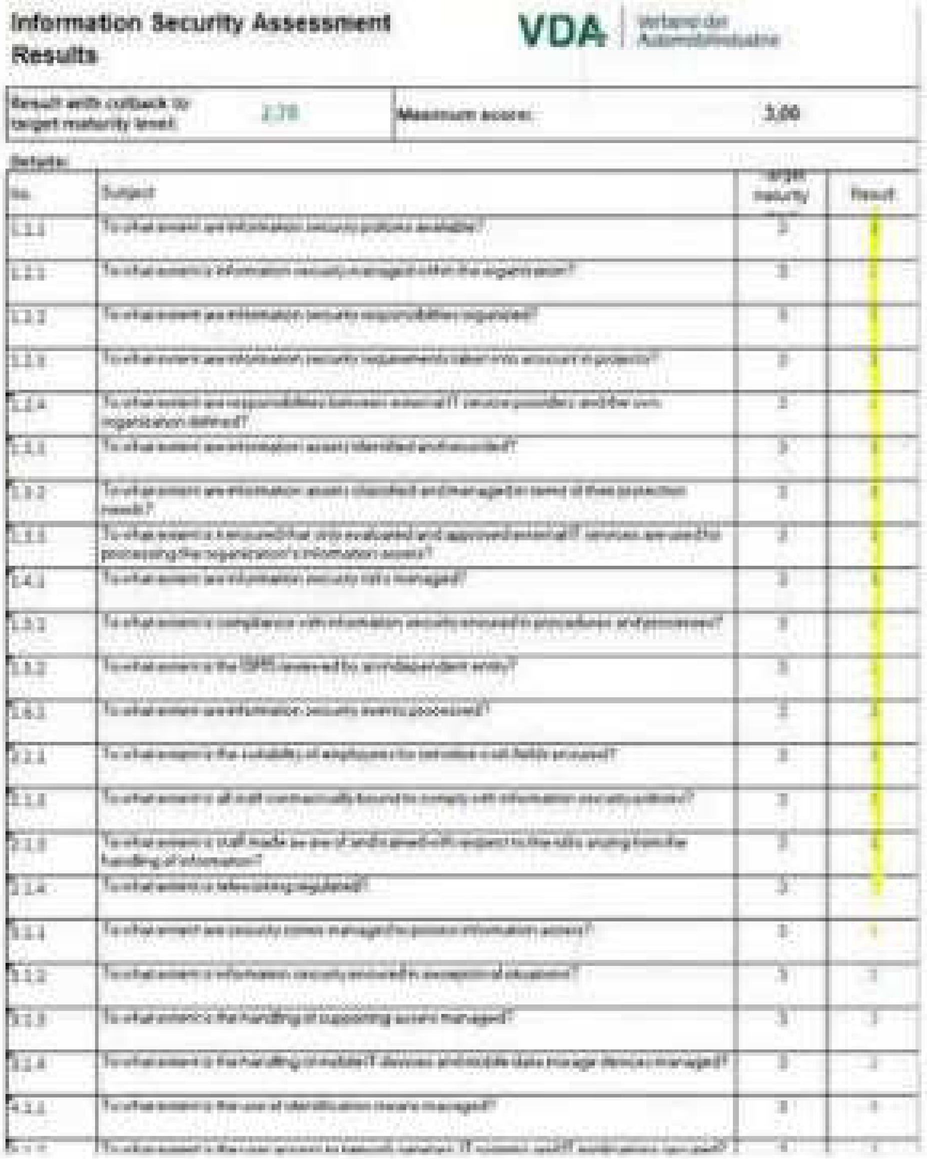
Tagged only for availability

Additional requirements
for high protection needs

+ The access rights are approved by the responsible internal Information Officer. (C, I, A)

Tagged for availability, integrity and confidentiality

Further recommendations: Handling the VDA catalogue



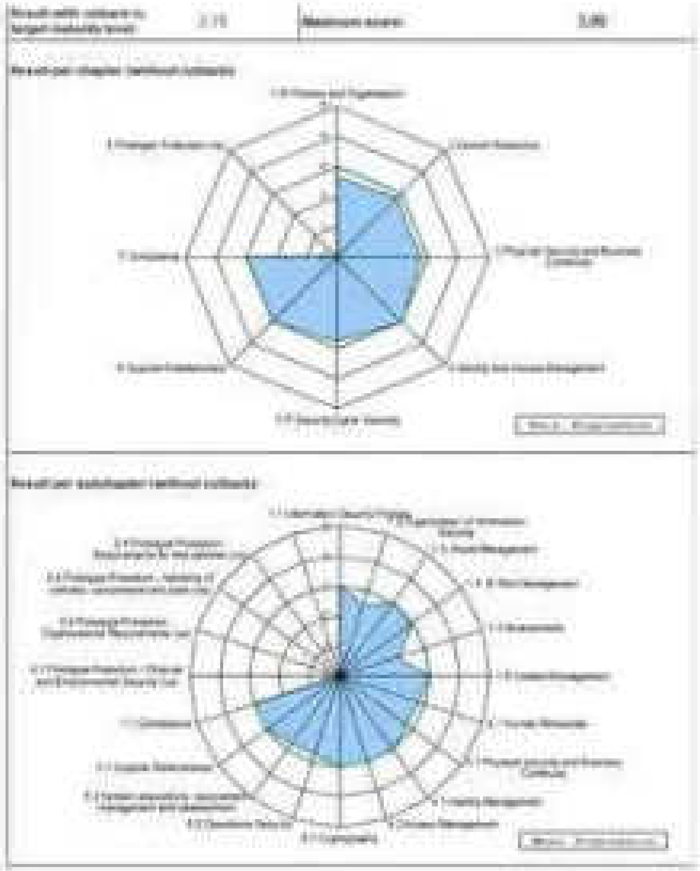
Information Security Assessment Results

VDA | Verband der Automobilindustrie

Result with cutback to target maturity level:	2,78	Maximum score:	3,00

Details:

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	[illegible]
1.2.1	To what extent is information security managed within the organization?	3	[illegible]
1.2.2	To what extent are information security responsibilities organized?	3	[illegible]
1.2.3	To what extent are information security requirements taken into account in projects?	3	[illegible]
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	[illegible]
1.3.1	To what extent are information assets identified and recorded?	3	[illegible]
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	[illegible]
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	[illegible]
1.4.1	To what extent are information security risks managed?	3	[illegible]
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	[illegible]
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	[illegible]
1.6.1	To what extent are information security events processed?	3	[illegible]
2.1.1	To what extent is the suitability of employees for sensitive work fields ensured?	3	[illegible]
2.1.2	To what extent is all staff contractually bound to comply with information security policies?	3	[illegible]
2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?	3	[illegible]
2.1.4	To what extent is teleworking regulated?	3	[illegible]
3.1.1	To what extent are security zones managed to protect information assets?	3	[illegible]
3.1.2	To what extent is information security ensured in exceptional situations?	3	[illegible]
3.1.3	To what extent is the handling of supporting assets managed?	3	[illegible]
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	3	[illegible]
4.1.1	To what extent is the use of identification means managed?	3	[illegible]
[illegible]	To what extent is the user access to network services, IT systems and IT applications secured?	[illegible]	[illegible]



Result with cutback to target maturity level:	2,78	Maximum score:	3,00

Result per chapter (without cutback):

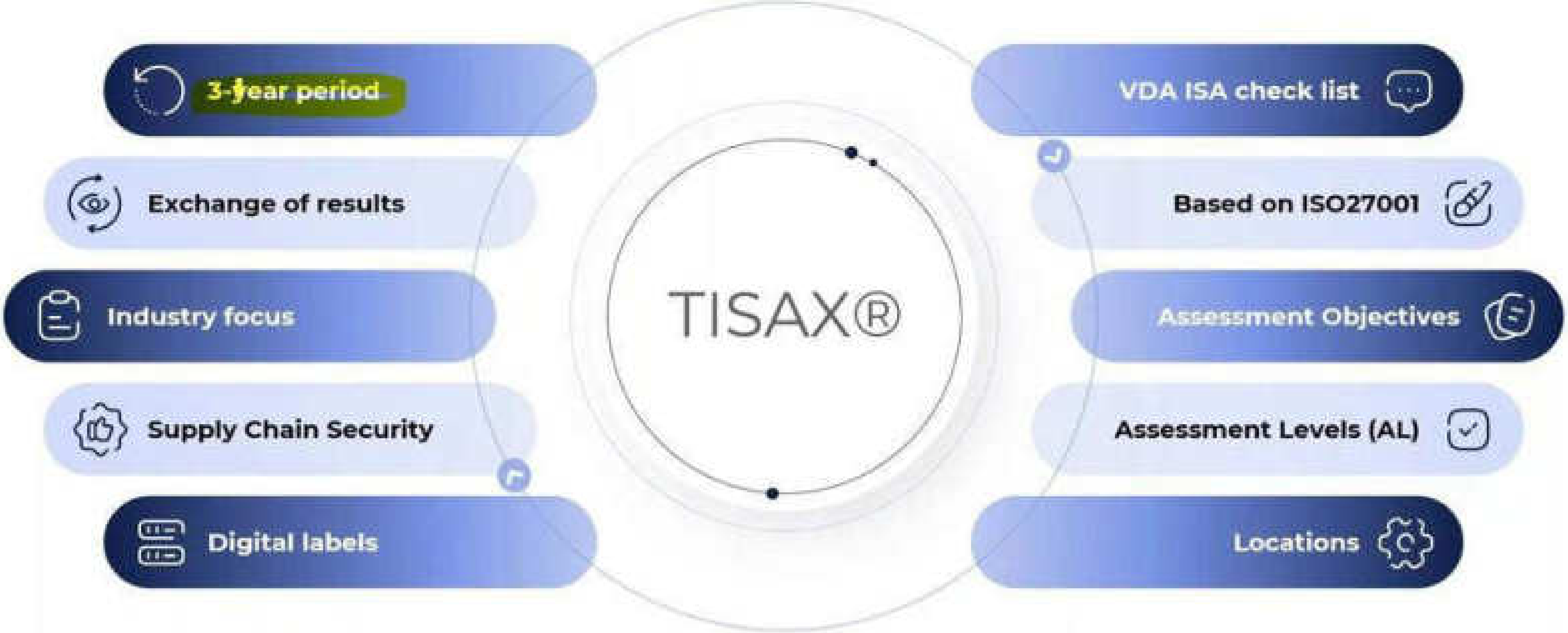
Result per subchapter (without cutback):

"Results" tab:

Here you can get your test result based on your own data entry.

2.7

2.1



TISAX®

3-Year period

Exchange of results

Industry focus

Supply Chain Security

Digital labels

VDA ISA check list

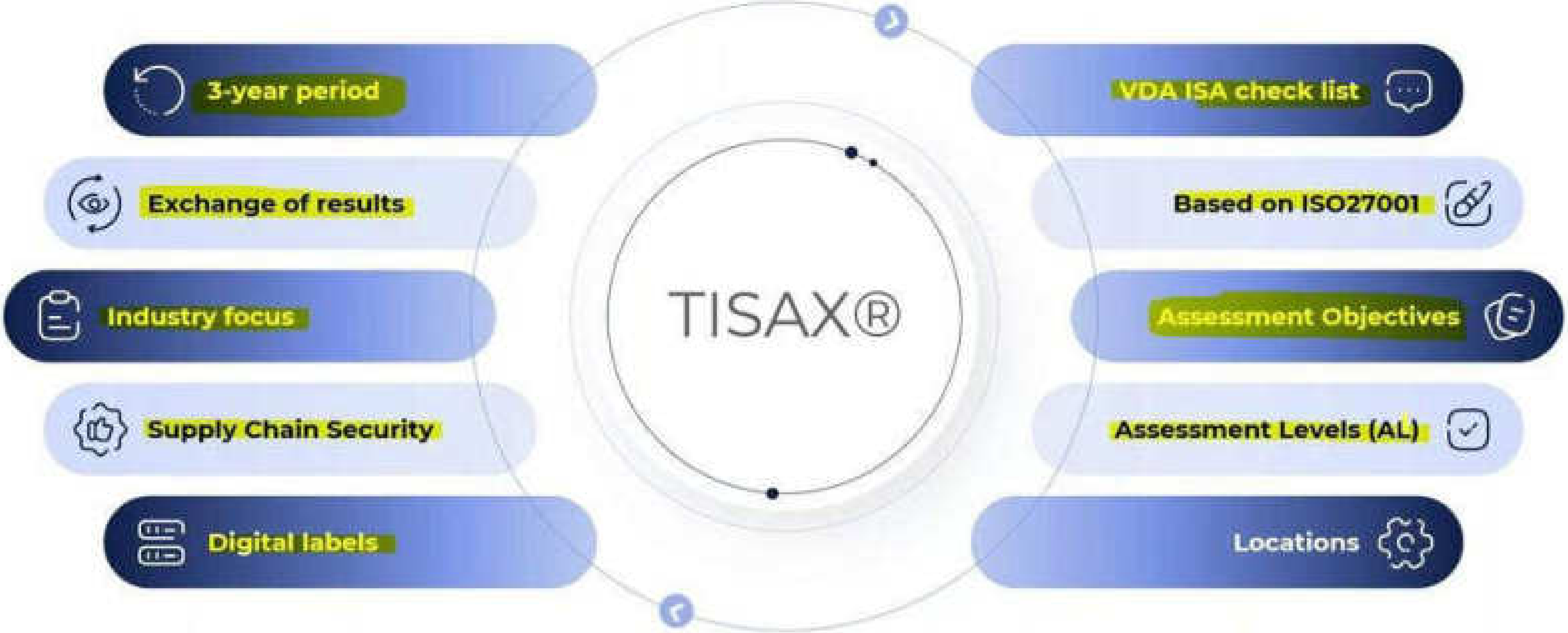
Based on ISO27001

Assessment Objectives

Assessment Levels (AL)

Locations

DNV



TISAX®

3-year period

Exchange of results

Industry focus

Supply Chain Security

Digital labels

VDA ISA check list

Based on ISO27001

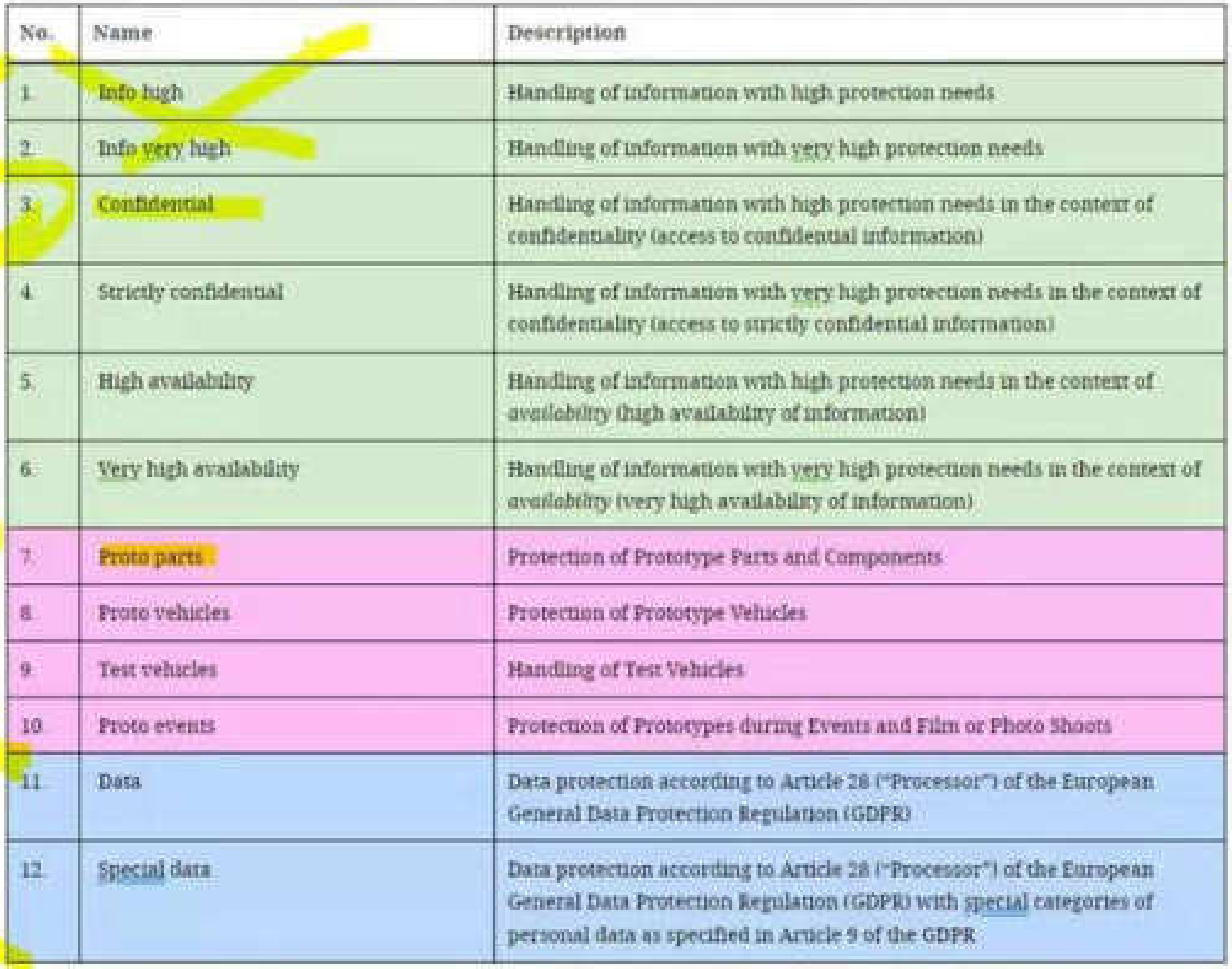
Assessment Objectives

Assessment Levels (AL)

Locations

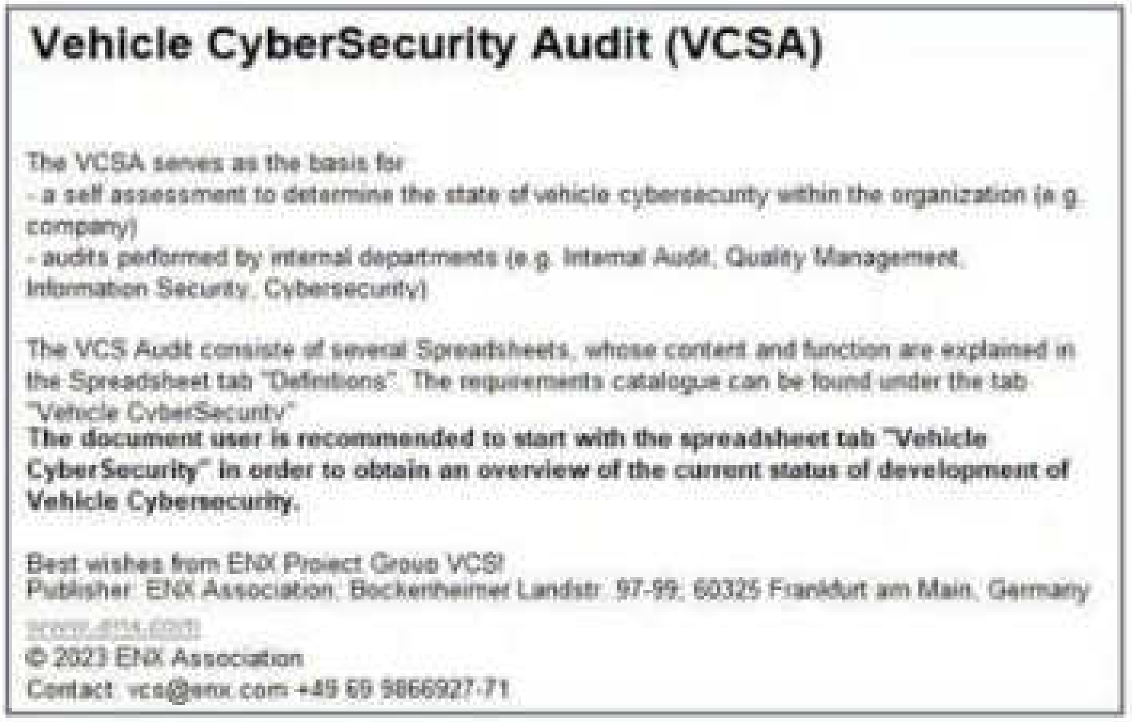
Q&A

Assessment objectives



	No.	Name	Description	
INFO SEC	1.	Info high	Handling of information with high protection needs	AL2
	2.	Info very high	Handling of information with very high protection needs	AL3
	3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information)	AL2
	4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information)	AL3
	5.	High availability	Handling of information with high protection needs in the context of *availability* (high availability of information)	AL2
	6.	Very high availability	Handling of information with very high protection needs in the context of *availability* (very high availability of information)	AL3
PROTO	7.	Proto parts	Protection of Prototype Parts and Components	AL3
	8.	Proto vehicles	Protection of Prototype Vehicles	AL3
	9.	Test vehicles	Handling of Test Vehicles	AL3
	10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots	AL3
DATA	11.	Data	Data protection according to Article 28 ("Processor") of the European General Data Protection Regulation (GDPR)	AL2
	12.	Special data	Data protection according to Article 28 ("Processor") of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR	AL3

New upcoming schemes

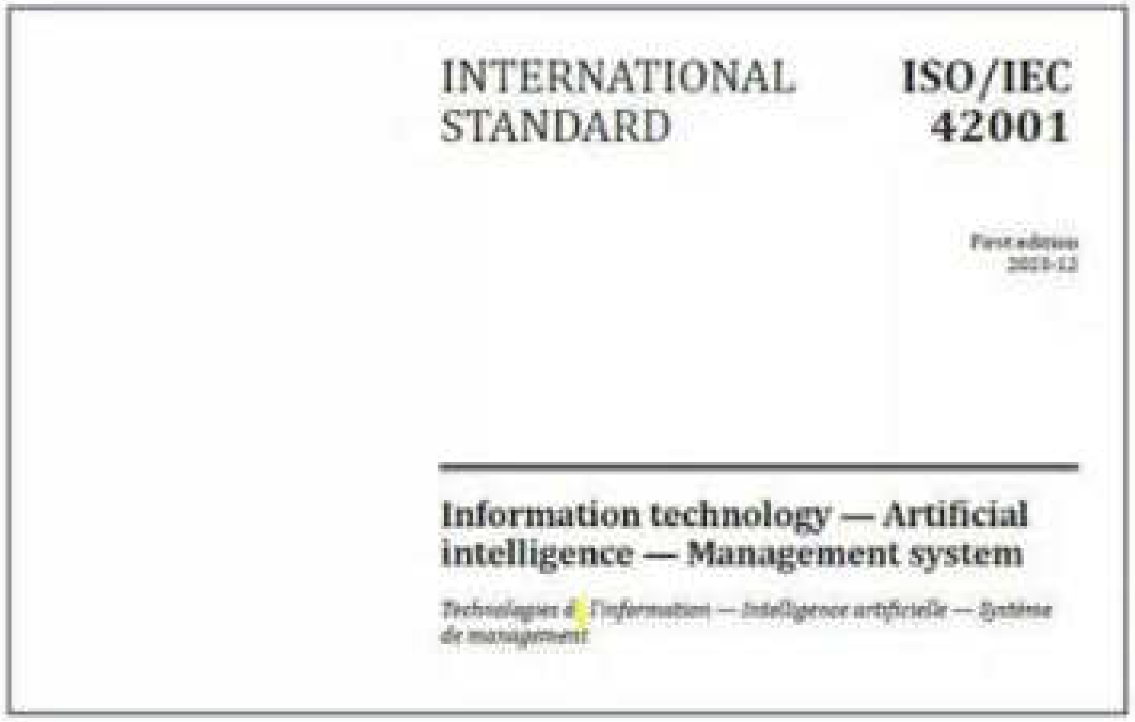


Vehicle CyberSecurity Audit (VCSA)

The VCSA serves as the basis for
- a self assessment to determine the state of vehicle cybersecurity within the organization (e.g. company)
- audits performed by internal departments (e.g. Internal Audit, Quality Management, Information Security, Cybersecurity)

The VCS Audit consiste of several Spreadsheets, whose content and function are explained in the Spreadsheet tab "Definitions". The requirements catalogue can be found under the tab "Vehicle CyberSecurity"
The document user is recommended to start with the spreadsheet tab "Vehicle CyberSecurity" in order to obtain an overview of the current status of development of Vehicle Cybersecurity.

Best wishes from ENX Project Group VCS!
Publisher: ENX Association, Bockenheimer Landstr. 97-99, 60325 Frankfurt am Main, Germany
www.enx.com
© 2023 ENX Association
Contact: vcs@enx.com +49 69 9866927-71



INTERNATIONAL STANDARD

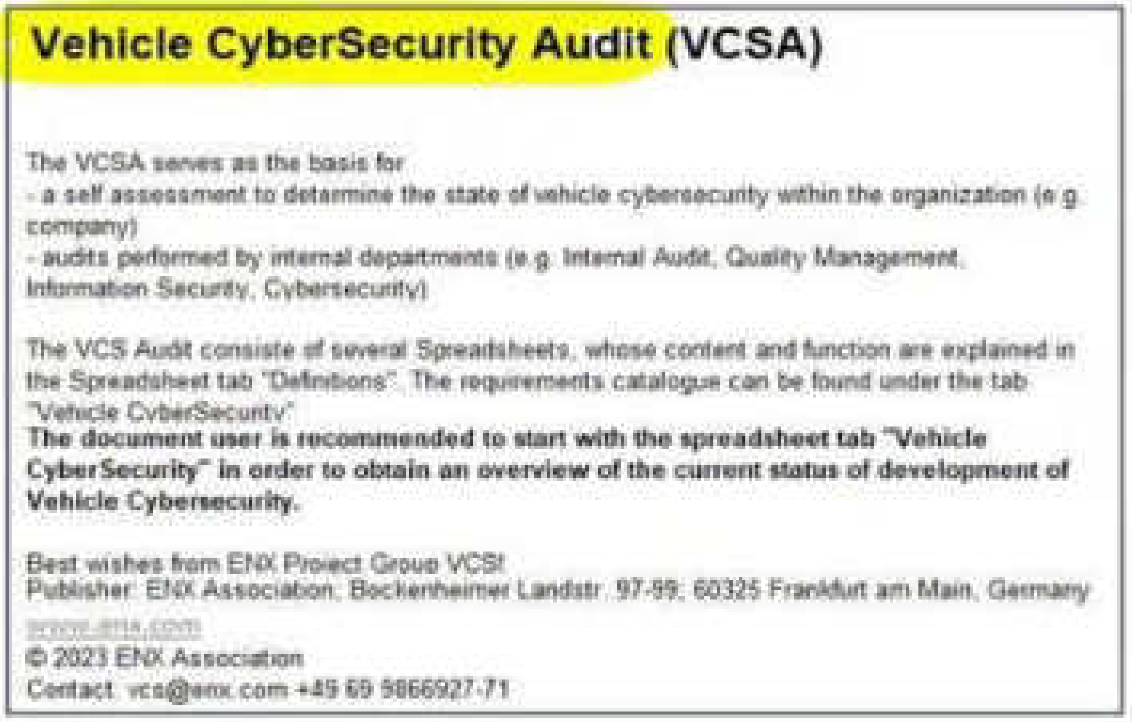
ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

New upcoming schemes



Vehicle CyberSecurity Audit (VCSA)

The VCSA serves as the basis for
- a self assessment to determine the state of vehicle cybersecurity within the organization (e.g. company)
- audits performed by internal departments (e.g. Internal Audit, Quality Management, Information Security, Cybersecurity)

The VCS Audit consiste of several Spreadsheets, whose content and function are explained in the Spreadsheet tab "Definitions". The requirements catalogue can be found under the tab "Vehicle CyberSecurity"
The document user is recommended to start with the spreadsheet tab "Vehicle CyberSecurity" in order to obtain an overview of the current status of development of Vehicle Cybersecurity.

Best wishes from ENX Project Group VCS!
Publisher: ENX Association, Bockenheimer Landstr. 97-99; 60325 Frankfurt am Main, Germany
www.enx.com
© 2023 ENX Association
Contact: vcs@enx.com +49 69 9866927-71

INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management