

TISAX[®]

BUREAU VERITAS

**TRUSTED INFORMATION
SECURITY ASSESSMENT
EXCHANGE**



**BUREAU
VERITAS**

CYBER ATTACKS: A REVOLUTION IN THE AUTOMOTIVE INDUSTRY

Cross-company recognition of the assessment results among all TISAX® participants

Contents

- P2/3 —
Introduction
- P4/7 —
TISAX® Overview and Advantages
- P8/11 —
Two Possible Roles in Terms of Participation
- P12 —
Tisax® Participant Exchanging Information
- P13 —
Tisax® Correlations With Iso/iec 27001
- P14 —
Evaluation Scheme Test Results
- P15 —
Tisax® Protection Level And A Assessment Objective (Assessment Levels)
- P16 —
Marking Level's Of Information (Label's Level)
- P17 —
Minimum Requirements For Prototype Protection
- P18 —
Location Classes And Check Types
- P19 —
Learn More About Highests Standards In Automotive Industry
- P20 —
About Bureau Veritas

In the era of digitization, information security is an increasingly decisive factor in remaining competitive.

This applies in particular to the automotive industry – here companies exchange a huge amount of sensitive data on a daily basis, data which needs to be protected against theft, loss or manipulation.

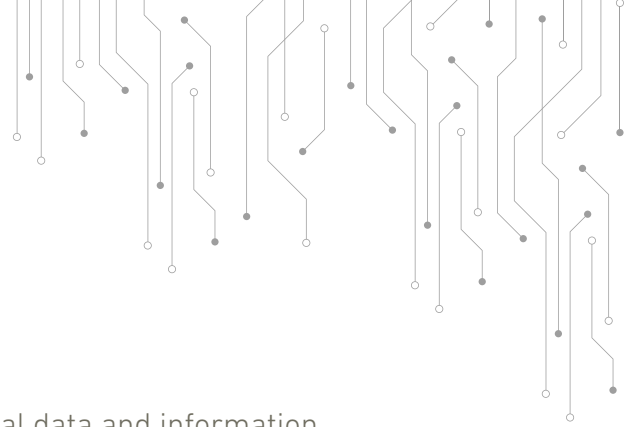
Suppliers and/or service providers for the automotive industry need to reassure customers that they keep their information secure.

Information security used to be considered as being the individual concern of each separate company, but this should change in the future through the common assessment and exchange mechanism TISAX® (Trusted Information Security Assessment eXchange).

TISAX® is a mark owned and property of ENX association.

Bureau Veritas is formally recognized by ENX as Audit Service to provide TISAX® Assessment audits.





Introduction

AUTOMOTIVE

Context and Information

Automotive players exchange and manage many types of digital data and information. Regardless of whether the data exchanged is internal data or client/supplier data, the necessity for protection is paramount.

Cyber Attack. A global threat

The automotive industry is a major target for hackers. This industry is one of the most advanced, in which the highest investments are made on the most innovative technologies.

With the expansion of new propulsion engines programs and autonomous vehicles technology, keeping the information safe is mandatory for all the industry players.

Companies that fail to protect themselves and their information against intrusion run a serious risk of jeopardizing their activities and revenues, as well as the security of their products.

Hackers are not only "digital pirates" but also organizations, competitors or states attacking organizations with the aim of damaging your performance and your business.

That is why it is mandatory for automotive players to demonstrate that they are protecting their data and that of their clients, suppliers and any other industry players with the most advanced management system organization.

What information must be protected?

Data related to parts definition

- Technical Specifications & parts definition
- Design and dimensional information
- Performance
- Validation (file PPAP/APQP)
- Homologation

Data related to the industrial relationship between client and supplier

- RFQ
- Contract information
- Parts tenders
- Scheduling
- Delivering
- Invoicing

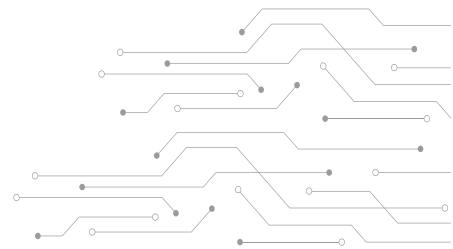
But Automotive players also need to take care of their **internal Digital information** which is of utmost importance in running their business.

Data used in the everyday running of the business

- Process, Industrial equipment information: Automated programs, Production and Maintenance Software
- Production Program
- Accounting
- Personal information
- Innovation, patterns, prototypes
- Embedded software for a part/system or function
- Information related to marketing & sales events or campaigns.

Information gathered => final customer information

- Final customer personal information: Address, phone number, e-mail, credit card information
- Final customer vehicle information: GPS information, mechanical information, electronic information, malfunction information, unusual aging, etc.



2 TISAX® OVERVIEW AND ADVANTAGES

PRINCIPLES

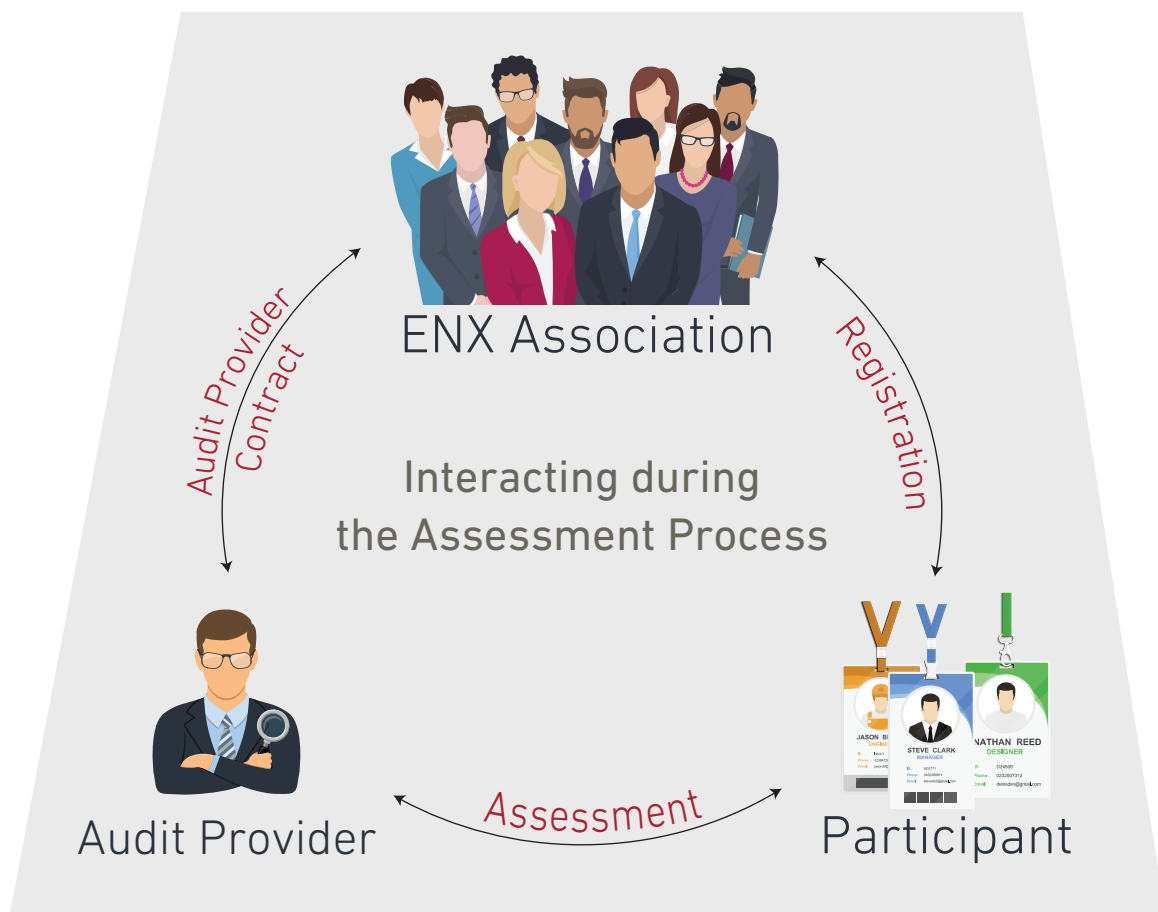
Firstly, the most important aspect is that TISAX® is a standard specifically aimed at the automotive industry. It does not consider any other industry and aims to protect automotive players' information security systems.

The second principle of TISAX® is to share the results. To demonstrate your performance in total transparency, TISAX® allows you to share your assessment results and the level of your information security management for incontestable recognition.

TISAX® is based on VDA-ISA Assessment with regard to information security requirements. It has been designed and built to respond to automotive players' requirements. Once the assessment has been performed and corrective actions implemented, you can use a dedicated digital platform to share your results and performance with any automotive players already registered on the TISAX® platform.

The players involved in the TISAX® assessment are:

- TISAX® association
- Audit Provider (ie: Bureau Veritas)
- Participant (company willing to be certified/assessed).



TISAX® Overview and Advantages

TISAX® CYCLE

Participation in the TISAX® Exchange automotive register is based on one assessment every 3 years. TISAX® Exchange automotive partners have confidential information that they need to share with their supplier and they want to be sure that the latter handles this information with the same due care.

The participants in TISAX® share information via a common online platform on the information security status of another participant, in the form of the results of assessments performed. Important to know: no TISAX® participant automatically has access to the assessment results of another participant. It is the audited company itself that decides who in the TISAX® network receives what information by explicit authorization to share the specified information on a case-by-case basis.

A few words about TISAX® & ENX:

The body responsible for TISAX® is the VDA and the ENX Association monitors the quality of execution and of the assessment results.

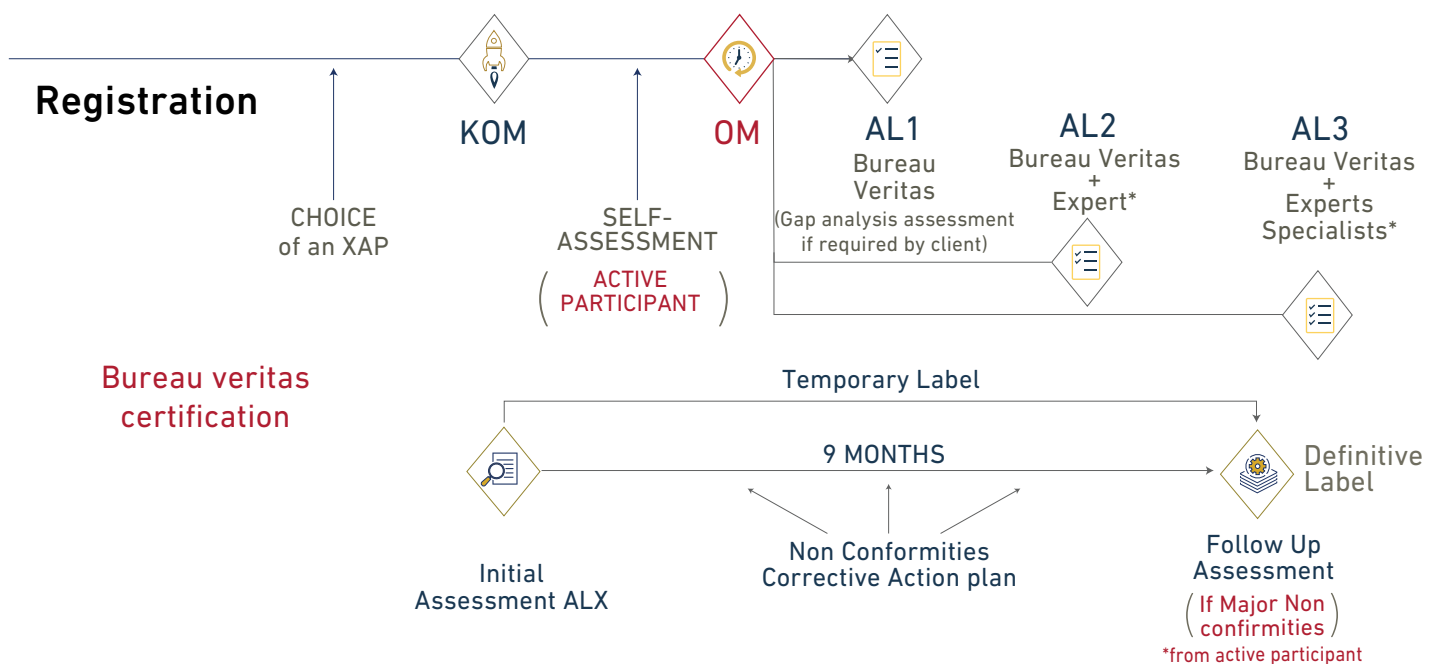
The ENX Association is an association of European vehicle manufacturers, suppliers and organizations, which was founded in 2000 according to the French law of 1901 on not-for-profit associations.

ENX members :

TISAX® is mostly supported by VDA members, the full list of which can be uploaded here. If you have a client within this member list, you may be required to be TISAX® assessed and Bureau Veritas can help you with that.

The overarching objective of TISAX® is to establish a standardized Label based on common criteria within the automotive industry and to create a sharing space/community where IT/IS performances are shared between automotive players.

TISAX® Assessment Flow Chart :



KOM - Kick-off Meeting

OM - Opening Meeting

AL - Assessment level

XAP - Audit Provider (i.e. Bureau Veritas)

TISAX® Overview and Advantages

THE SIX STAGES IN GAINING TO OBTAIN TISAX®

By Bureau Veritas Certification

01 Action:
Registration on TISAX® platform + Choice of Audit Providers (i.e. Bureau Veritas).

Document: SF01 TISAX® register
Prepare: Customer
Confirm: BVC



02 Action:
Preliminary Verification of Label/Scope Assessment (Evaluation scheme), Information protection class, Simplified Group Assessment (if possible) and Signing contract

Document: Contract Label / Scope Assessment
Prepare: Customer
Confirm: BVC



03 Action:
Self-Assessment (AL1)

Document: VDA-ISA.xls
Organization documentation
Prepare: documentation
Confirm: BVC



04 Action:
Off-Site Audit (Review performance of the assessment AL1, using documentation and Confirmation of Label/Scope Assessment) or on-site audits (AL2)

Document: VDA-ISA.xls
Organization documentation
Prepare: BVC
Confirm: ENX



05 Action:
On-Site Audit (AL3)

Document: VDA-ISA.xls
Organization documentation.
Prepare: BVC
Confirm: ENX



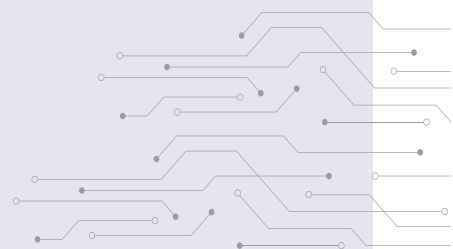
06 Action:
Label Confirmation.

Prepare BVC:
Confirm: ENX



07 Action:
Exchange of information on the results of the audit with other selected TISAX® participants, based on explicit authorization by the audited company

Document: TISAX® Excerpt or TISAX® SF01
Prepare: BVC
Confirm: Customer



TISAX® Overview and Advantages

BENEFITS OF TISAX®

This cooperation creates value, responds to the need to protect information appropriately, and provides the following benefits:



Cross-company recognition of the assessment results amongst all TISAX® participants



Broad acceptance in the automotive sector



Only one TISAX® assessment every three years



Effective risk management strategies



Higher credibility for certified organization between suppliers and customers



Mutual recognition in the TISAX® network saves time and cost



Eliminates the need for multiple checks



Better clarity due to harmonized VDA-ISA test catalog



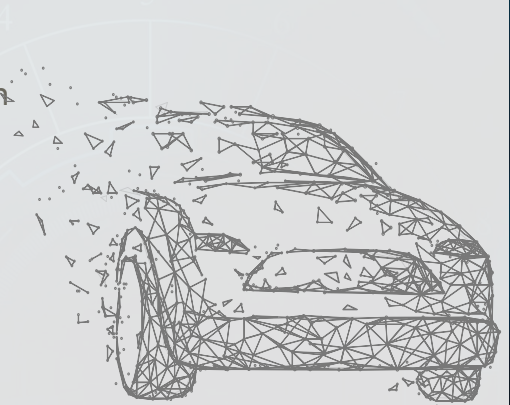
Complete control of the assessment results



Consolidates existing business relationships and facilitates new ones



Consequent orientation to customer needs



3 TWO POSSIBLE ROLES IN TERMS OF PARTICIPATION

There are two roles within the exchange model, which each participating company can take on according to its needs:



Passive participant (e.g. OEM, automotive manufacturer): Calls for another company (e.g. a supplier) to undergo an assessment and requests access to the assessment results.



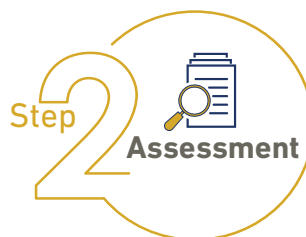
Active participant (e.g. supplier): A company is either called by another company (e.g. OEM or customer) to undergo an assessment, or undertakes to have an called upon by assessment done on their own initiative. After completion, the active participant makes it possible for selected companies (e.g. OEMs) to gain access to the assessment results.

For Participants, there are 3 steps to follow in this specific order

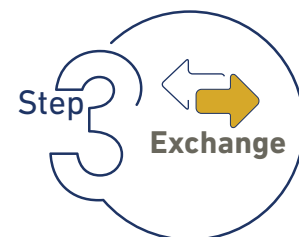
The 3-step TISAX® process consists of the following steps:



ENX gathers information about your company and what should be included in the assessment.



The assessment(s), conducted by one of TISAX®-formally recognized audit providers. BV is one of the audit providers.



Share the results of assessments/certification with interested parties.

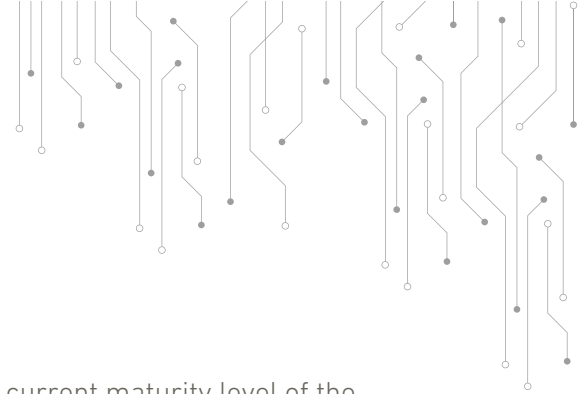
The Step 1 needs to be done by the Client on the TISAX® platform. There is a specific process to be followed in order to get a "Participant number".

During the online registration process:

- ENX asks candidate participants for contact details and billing information.
- Candidate participants have to accept TISAX® terms and conditions.
- Candidate participants define the scope of their information security assessment.

In Step 1, the definition of audit scope is based on the VDA-ISA catalog. Depending on this selection, the audit duration will be calculated. It cannot be pre-calculated based solely on the structure of the organization.





In Step 2 can be subdivided into 4 steps:

a) Assessment preparation

Prepare the assessment. The extent of the assessment depends on the current maturity level of the information management system. It has to be based on the VDA-ISA catalog.

b) Audit provider selection

Once Participant is ready for the assessment, Participant choose one of the ENX's recognized Audit providers for TISAX® assessment audits. Bureau Veritas can be chosen even if it is not yet on the website since it is currently in the process of being formally accredited. BV will be visible on the website when the 1st Pilot audit has been completed.

c) Information security assessment(s)

The audit provider will conduct the assessment based on an assessment scope that matches your partner's requirements. The assessment process will consist of an initial audit at the very least. If the Participant's company does not pass the assessment right away, the assessment process will consist of an initial audit at the very least.

d) Assessment result sharing

Once the Participants have passed their assessment(s), the audit provider will provide the Participants with the assessment results and report.



Step 3 Sharing the results on the TISAX® platform with the Participant's partners (clients): the assessment results can be shared with the Participant's partners (clients). The content of the TISAX® report is structured in levels. Participants can decide the level up to which their partners have access.

The TISAX® label is officialized by the ENX organization through the publication of the results and Assessment Label on the ENX digital platform.



SCOPE OF ASSESSMENT

There are 3 different assessment scopes to choose from:

● **Standard Scope**

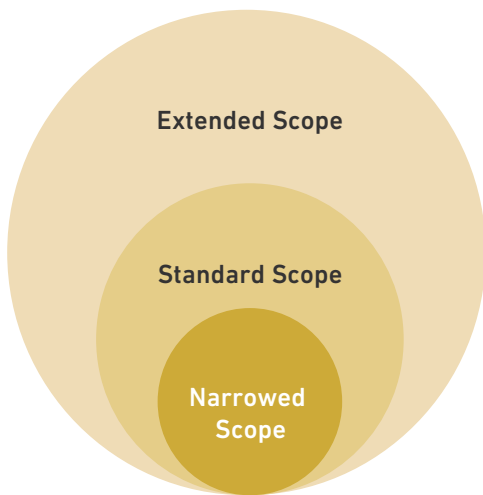
It is a pre-defined scope; it comprises all processes and resources involved in collecting, storing and processing information

● This is the choice in the majority of cases

● **Custom Scope**

● Extended scope: Wider than Standard Scope

● Narrowed Scope: Reduced from Standard scope



“TISAX® assessment labels” are a concept to summarize the assessment result and are the output of the TISAX® process. There are 4 different labels that partners (Clients) can request that participants be assessed on.

Assessment objectives are defined at the beginning of the process and will become an assessment level once the audit is performed.

Each label can be either " high" or "very high" to define the protection level reached.

Figure 5: Scope types: extended scope, standard scope, narrowed scope

No.	VDA-ISA criteria catalog	Protection level (PL)	TISAX® assessment objective	AL
1.	Information security	PL high	Information with high protection level	AL 2
2.	Information security	PL very high	Information with very high protection level	AL 3
3.	Prototype protection	PL high	Handling of prototypes with high protection level	AL 2
4.	Prototype protection	PL very high	Handling of prototypes with very high protection level	AL 3
5.	Data protection	PL high	Data protection according to German §11 BDSG (“Auftragsdatenverarbeitung”)	AL 2
6.	Data protection	PL very high	Data protection with special categories of personal data .Special categories according to German §3 section (9) BDSG (“Besondere Arten”), Data Protection according to German §11 BDSG (“Auftragsdatenverarbeitung”)	AL 3

In each case, the scope and duration of the TISAX® assessment are determined according to the list of criteria to be dealt with, the objectives of the protection, the complexity of the ISMS and the number of sites involved.

VDA-ISA SPECIFIC Requirements

The VDA-ISA assessment has a generic questionnaire on Information security and 3 additional specific topics which are :



Prototype Protection



Information Security



Data protection

The “**Prototype protection**” module has been revised and now follows the same structure as the main catalog. Originally, this items was covered by VDA PTS.

The “**Information Security**” This module describes the specific requirements to be respected within the organization to protect Automotive related projects/products from TISAX®/ENX Stakeholders.

The “**Data protection**” module applies when service providers are mandated to process information encompassed by Art. 28 of the European General Data Protection Regulation (GDPR).

VDA-ISA Example Assessment

Information Security Assessment - Questions		VDA	Verband der Automobilindustrie
based on ISO 27001:2013			
Company:	0		
Location:	0		
Date:	00/01/1900		
Maturity level Level 0-5; na	In case a question does not apply, please insert na (not applicable).		
1 General aspects			
<input type="text"/>	1.1 To what extent is an Information Security Management System approved by the organization's management and is its scope documented. (Reference to ISO 27001: 4 and 5.1)		
Objective:	Systematic control and review of information security within the specified scope is effected by means of the establishment, operation and further development of an Information Security Management System (ISMS) and the assignment of responsibilities. The ISMS must define processes and procedures in order to achieve the information security objectives with respect to adequate confidentiality, availability and integrity of the company assets based on the security policy.		
Requirements:	<p><u>This must include:</u></p> <ul style="list-style-type: none"> + The organization's requirements for an ISMS are determined. + An ISMS approved by the organization's management is established. + The scope of the ISMS is specified (e.g. organization in whole or in part). + A Statement of Applicability (SoA) is provided (e.g. filled-in VDA ISA catalogue). <p><u>This should include:</u></p>		

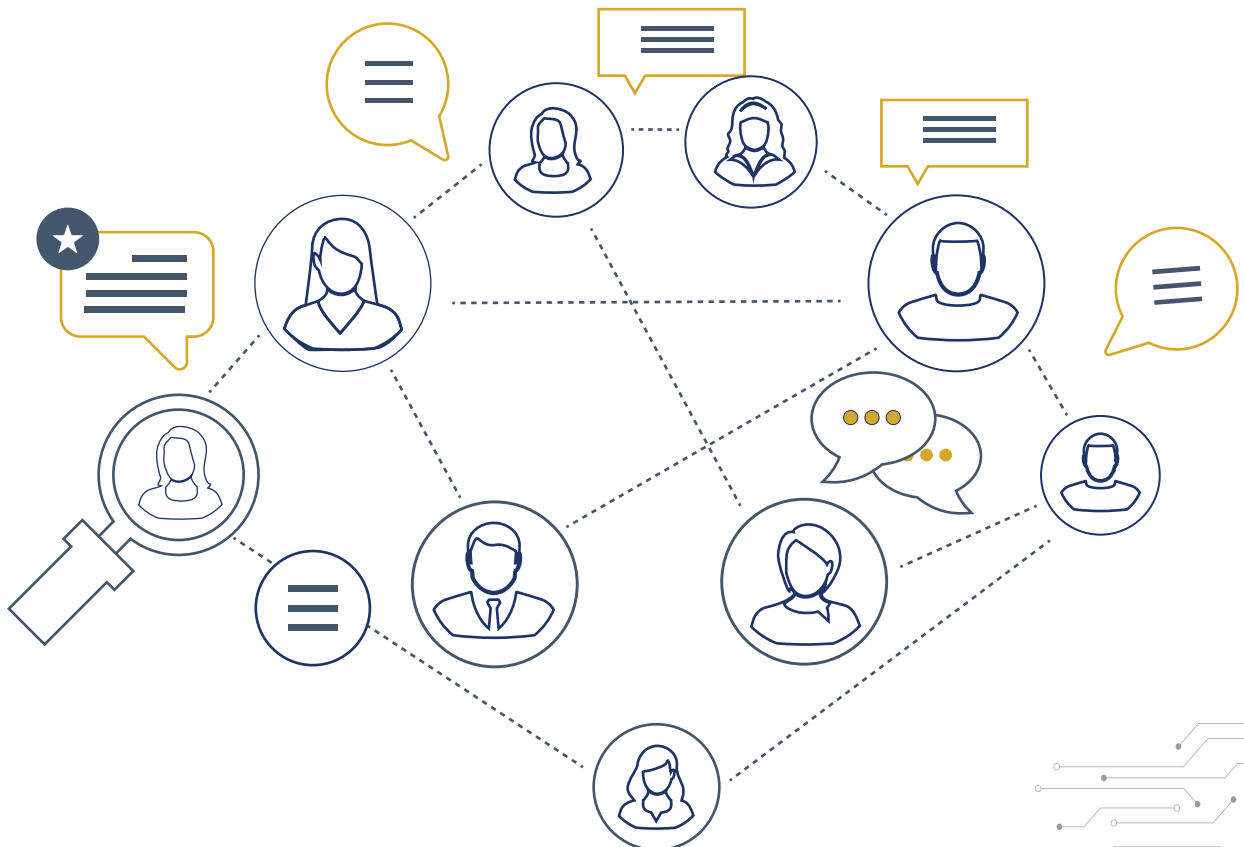
4

TISAX® PARTICIPANT EXCHANGING INFORMATION

Access to TISAX® is via a subscriber registration, which takes place online on the TISAX® portal. Registration is the prerequisite for being able to select a TISAX® accredited audit service provider. Registered participants will receive a list of accredited providers from which they can freely choose. An organization may also register several locations and have a group assessment carried out. After the assessment based on VDA-ISA, information can be provided or obtained in TISAX®. Who is behind TISAX®?

TISAX® uses the VDA-ISA questionnaire compiled by the German Automotive Industry Association VDA based on essential aspects of ISO/IEC 27001.

ENX monitors adherence to the TISAX® procedure, which includes general requirements for audit service providers and specific requirements for ENX TISAX® audit service providers, and safeguards the quality of implementation and assessment results. To this end, ENX concludes contracts with all authorized audit service providers as well as and the participants. Standardization and quality control will ensure common recognition of the testing.



5

TISAX® CORRELATIONS WITH ISO/IEC 27001

Companies in the automotive industry have to demonstrate at regular three-year intervals that they fulfil the required security criteria of their sector.

The basis for this proof is the VDA-ISA catalog of requirements issued by the Association of the Automotive Industry (Verband der Automobilindustrie, VDA). The VDA-ISA catalog comprises the key aspects and criteria of the internationally recognized standard ISO/IEC 27001 and additional lists of criteria, which specifically apply to the automotive sector, such as the involvement of third parties and the protection of prototypes.

Furthermore, there is a fully developed and comprehensive audit and exchange mechanism. The audit and reporting processes ensure a high degree of comparability and transparency and thus strengthen the feeling of confidence of the respective customers who are therefore demanding to an increasing extent the attainment of the relevant TISAX® labels respective customers. As a result, these customers are increasingly demanding that the attainment of the relevant TISAX® labels should be a binding requirement.. The TISAX® online platform makes it possible for participants to exchange assessment data and at the same time makes it easier for participants and audit providers to get in touch with one another.

Thus, it can be said that the VDA has installed a parallel certification world for information security in the automotive industry with ENX and the TISAX® examination process. A fundamental difference also exists in the consideration of information security. ISO/IEC 27001 focuses on an organization's own information security (as well as regulations concerning processes outside of the organization's own ISMS and documents supplied by third parties). But TISAX® has a very deep focus on the security of third-party information in an organization's own ISMS. This is also reflected in the risk analysis.

A company that registers in TISAX® has almost worked out a complete ISMS according to ISO/IEC 27001, which it will normally be able to confirm without much additional effort with an internationally recognized ISO/IEC 27001 certification. If it is an automotive supplier, it also has to provide evidence of "Prototype protection", "Data protection" and "Connection to the third party" for supplier approval.



Share
assessment
results

Execution
of Assessment

Select Audit
Provider

Register

6

EVALUATION SCHEME TEST RESULTS

The assessment begins with a basic examination of the "Information Security" topic, and may be extended to the optional modules of "Connection to third parties", "Data protection" and "Prototype protection".







The VDA-ISA "Information Security" questionnaire includes 52 security topics (controls) based on ISO/IEC 27001, evaluated using SPICE ISO 15504, which gives the company a comprehensive overview of the state of its own information security. Each of these topics must have a degree of goal achievement (from level 0 to 5) to obtain an overall rating.

A degree of goal achievement (from level 0 to 5), so to get overall rating.

The [VDA-ISA questionnaire](#) uses the measures from Annex A of ISO/IEC 27001. These were formulated as questions and must be evaluated by the company itself with a maturity level of "1" to "5".

The actual evaluation of the results is carried out mathematically, whereby testing is always carried out against the mean target maturity level of "3".



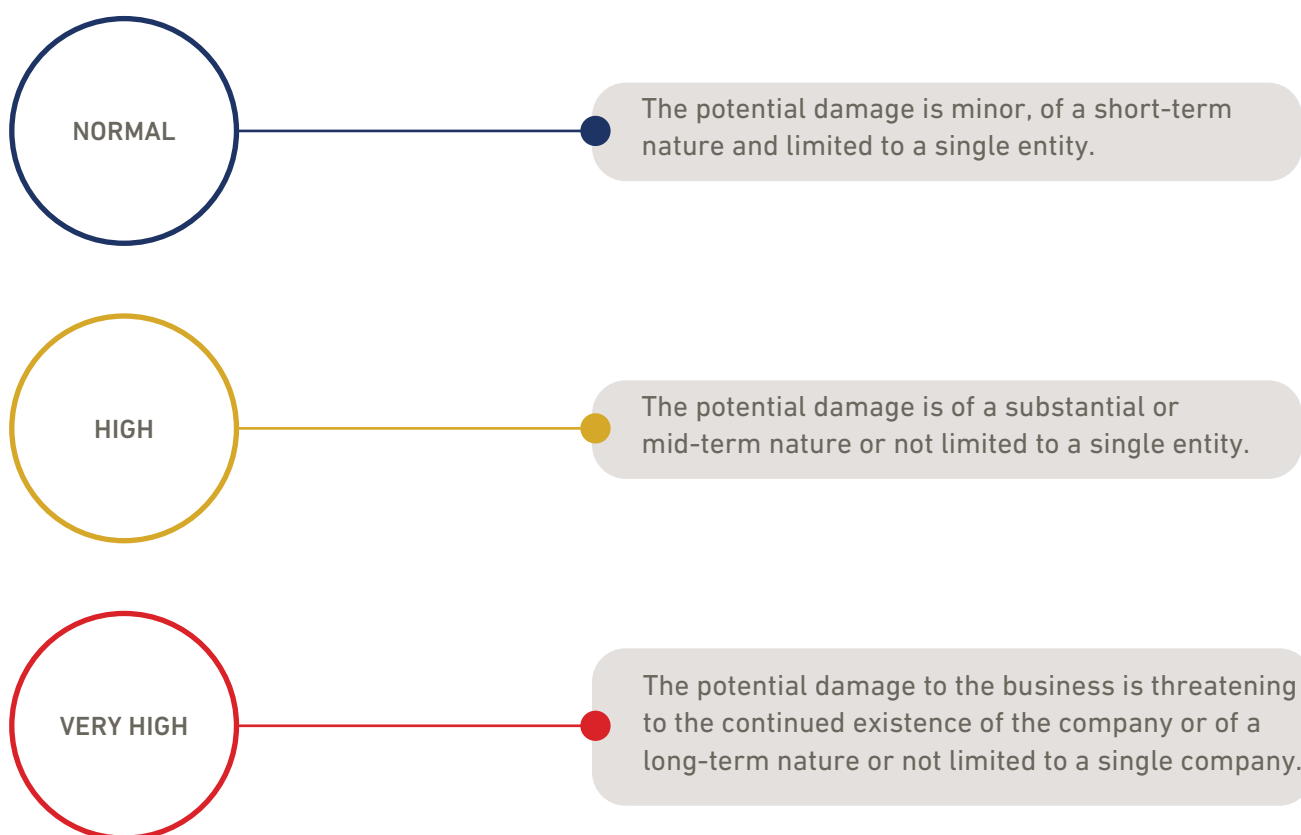
MATURITY LEVEL	DESCRIPTION
 Incomplete	There is no control, or it does not work.
 Performed	There is a control, but it is not documented, and nobody knows about it.
 Managed	There is a control and it is documented, but not completely updated, or not 100% in line with the reality.
 Established	There is a control and it is documented, completely updated, in line with the reality.
 Predictable	Level 3, with the addition of Key Performance Indicators (KPIs)
 Optimizing	Level 4, with the addition of specific improvements to the control.

7

TISAX® PROTECTION LEVEL AND ASSESSMENT OBJECTIVE

(Assessment levels)

The ENX Association, as the operator of the TISAX® program, has clearly defined different levels and scopes of assessment. TISAX® differentiates between three different “protection levels” (normal, high and very high), defining the required level of protection of the information in question.



Furthermore, TISAX® differentiates three “assessment levels (AL)” defining the depth of assessment and the assessment method:

- Information with **normal protection level: Assessment level 1** in the form of self-assessment. Results of assessments with assessment level 1 are normally not used in TISAX® but may be requested outside the scheme.
- Information with **high protection level: Assessment level 2** through an audit organization, using the self-assessment as a basis, as well as various documents and a telephone interview (if required, on site inspection).
- Information with **very high protection level: Assessment level 3** carried out by an independent audit provider on the basis of documentation and an on-site audit.

8

MARKING LEVELS OF INFORMATION (LABEL'S LEVEL)

Proper labeling is a prerequisite for proper handling of information. Therefore, information should be labeled according to its classification level.

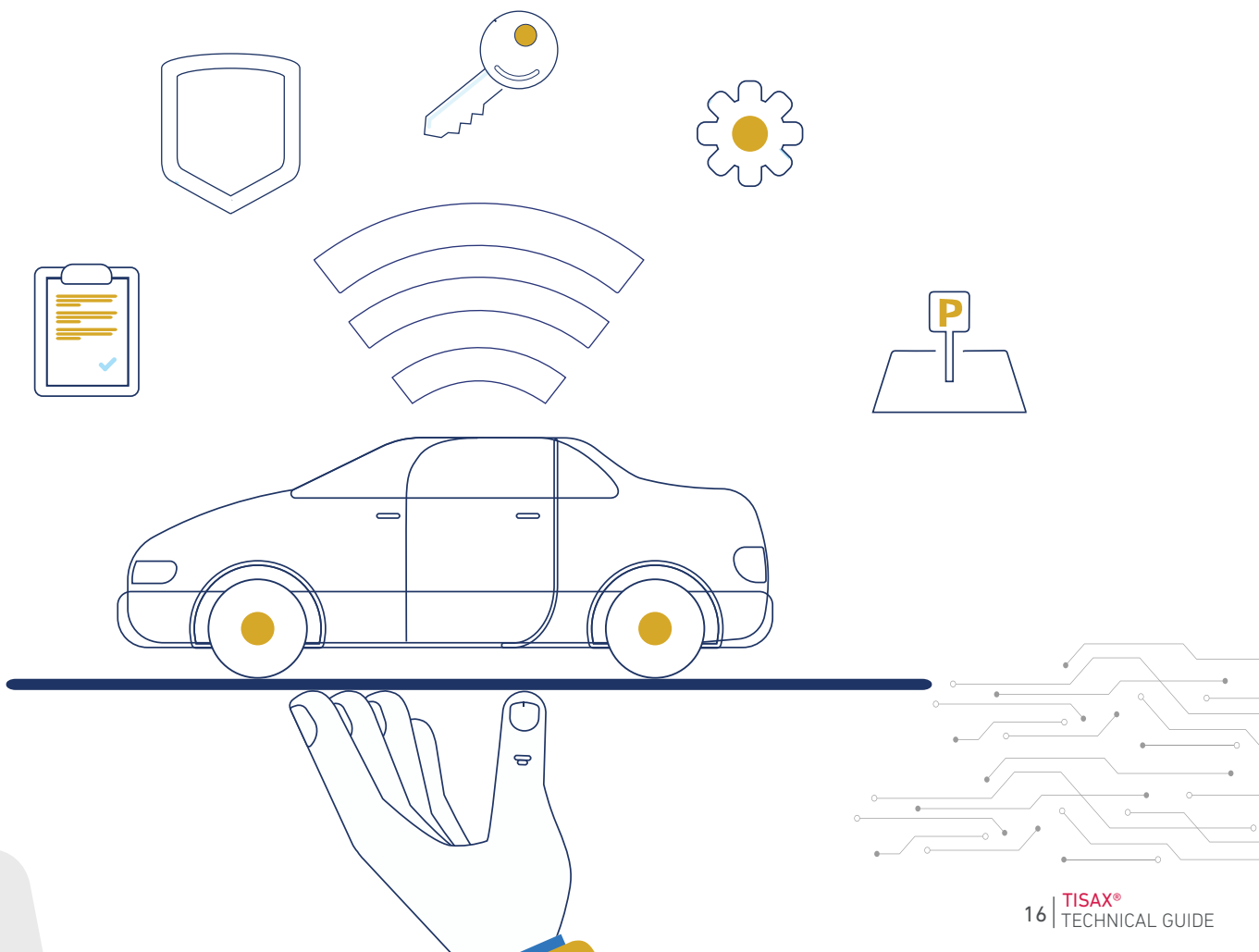
In addition to the creator, both recipients and processors of information must know, understand, and apply the classification levels and associated requirements for handling this information.

In particular, in the transmission of confidential and strictly confidential information across company boundaries (eg to partner companies) labeling is mandatory. When labeling, the Table 3 of the information and its classification level must be taken into account.

In addition to the uniform scheme for information classification and the corresponding labeling in the document, the Information Security Working Group focuses on uniform labeling for IT applications in particular. For example, a color hint when opening digital information (e.g. e-mail, presentation file) is an important sensitizing feature.

This gives the recipient a visual clarification of the classification level of the digital information.

In addition, a colored reference (e.g. in the form of a colored bar) creates a uniform understanding of the classification level, irrespective of country and language-specific differences.



9

MINIMUM REQUIREMENTS FOR PROTOTYPE PROTECTION



CONDITIONS

TARGET GROUP

01

Physical and environmental security

All companies that manufacture, store or leave vehicles or components classified as vulnerable on their premises.

02

Organizational requirements

All companies that manufacture or supply vehicles or components classified as vulnerable.

03

Handling vehicles, components or components classified as vulnerable

All companies that manufacture or supply vehicles or components classified as vulnerable.

04

Requirements for test vehicles

All companies that manufacture or leave test vehicles classified as vulnerable on their premises.

05

Requirements for events and shootings

All companies involved in the planning or preparation of events or shootings with vehicles or components classified as vulnerable.



10 LOCATION CLASSES AND CHECK TYPES

In the regular process, every location is subject to the same intensity, assessment methodologies, etc. (of course depending on the assessment objective). In the simplified group assessment process there are now three different classes of locations which are each subject to a different type of “check”. All locations must be part of the assessment scope, regardless of their class.

Location classes and check types

Location class	Check type	Abbreviation
Main location (headquarters)	Precondition check	PCC
Sample location	Sample check	SAC
Main location (headquarters)	Simplified check	SIC

Check type differences

Check type	Additional requirements	Assessment level	Locality
Precondition check	Yes	Always AL 3	Always “On site”
Sample check	Yes	AL 3 or AL 2	“On site” or “Remote”
Simplified check	Yes	AL 2 or AL 1	“On site” or “Remote”



Additional requirements:

The additional requirements cover the central processes. They vary slightly over the location classes. At the main location, the audit provider focuses on the role of the headquarters as the hub of the ISMS. For the other locations, the audit provider focuses on how predictably and reliably they interface with the hub.



Assessment level:

For the main location, the assessment level is always AL 3. For sample locations, the assessment level can be either AL 3 or AL 2. For the remaining locations, the assessment level can be either AL 2 or AL 1



Locality

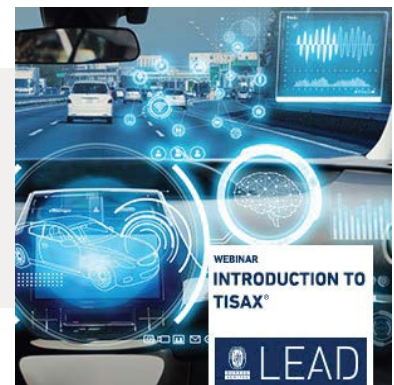
The precondition check is always conducted “on site”. For the other check types, the locality is derived from the requirements that come with the respective assessment objective. Example: For both prototype assessment objectives, the locality must be “on site”.

LEARN MORE ABOUT THE HIGHEST STANDARDS IN THE AUTOMOTIVE INDUSTRY



Discover our e-Learnings and Self-assessment tool relative to IATF 16949 (the new Automotive Quality Management System Standard).

Get informed thanks to our Webinar on TISAX®, the Information Security Management Standard in the Automotive industry.



Learn about the VDA 6.3 Process Audit and how to implement and evaluate your industrial performance in relation to German Automotive players.

HOW TO GET MORE INFORMATION?

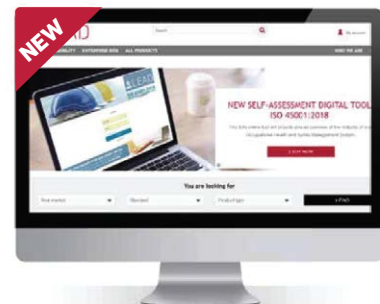
SHARE YOUR QUESTIONS AND DISCUSS THEM WITH YOUR CONTACTS ON **LINKEDIN** AND **TWITTER**

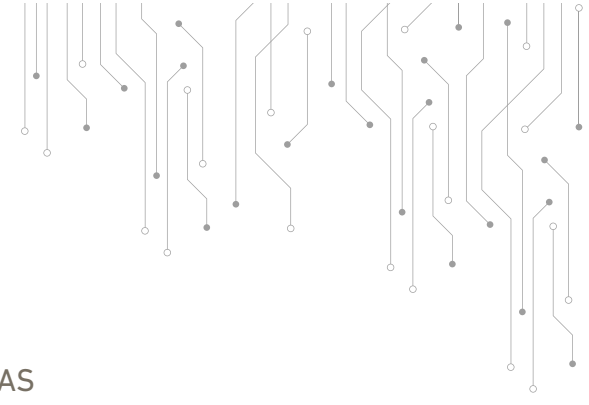


Follow us on Twitter
@LEAD_BV



Join our community
Bureau Veritas Certification





ABOUT BUREAU VERITAS

Bureau Veritas is a world leader in testing, inspection and certification. We help clients across all industries address challenges in quality, health & safety, environmental protection, enterprise risk and social responsibility.

We support them in increasing performance throughout the life of their assets and products and via continuous improvement in their processes and management systems.

Our teams worldwide are driven by a strong purpose: to preserve people, assets and the environment by identifying, preventing, managing and reducing risks.

WHY CHOOSE BUREAU VERITAS?



Deep knowledge of the regulation and the industries of our clients



World leader in inspection and certification



Technical expertise in over 140 countries



Effective international network

For more information, contact Bureau Veritas:

Le Triangle de l'Arche
8 cours du Triangle
CS 90096
92937 Paris La Défense Cedex
FRANCE

bureauveritas.com

contact.lead@bureauveritas.com