

ASSESSMENT · AUTOMOTIVE

TISAX: Information security for the auto industry

If you work for German carmakers or their large suppliers, you will be asked about TISAX as soon as confidential development data or prototypes are involved.

OPERATOR	BASIS	RESULT	VALIDITY
ENX Association	VDA ISA (Information Security Assessment)	TISAX label, not a certificate	3 years

In brief

TISAX stands for Trusted Information Security Assessment Exchange. The scheme is run by the ENX Association, a body formed by the European auto industry. Assessments follow the ISA (Information Security Assessment) catalog published by the German Association of the Automotive Industry (VDA). It is modeled on ISO/IEC 27001 and adds requirements for prototype protection and data protection.

What you get at the end is not a certificate. It is an assessment result with one or more labels, and it is not public. You share it through the ENX portal with the specific customers who need to see it. The result is valid for three years.

The assessment levels set how deep the audit goes. At AL 1 the auditor only checks that a self-assessment exists; TISAX does not use this level. At AL 2 the auditor checks the self-assessment for plausibility, reviews evidence and holds an interview, usually by video call. At AL 3 the audit is thorough, with documents, interviews and an on-site visit.

LABEL (ASSESSMENT OBJECTIVE)	WHAT IT COVERS	ASSESSMENT LEVEL
Confidential	information with a high protection need	AL 2
Strictly confidential	information with a very high protection need	AL 3
High availability	high availability, for example for series parts	AL 2
Very high availability	very high availability	AL 3
Proto parts	prototype parts and components	AL 3
Proto vehicles	prototype vehicles	AL 3
Test vehicles	test vehicles	AL 2

LABEL (ASSESSMENT OBJECTIVE)	WHAT IT COVERS	ASSESSMENT LEVEL
Proto events	events and photo shoots with prototypes	AL 2
Data	personal data	AL 2
Special data	special categories of personal data	AL 3

Depending on the label, AL 2 or AL 3 is required. The table follows the current TISAX Participant Handbook from ENX. Some older sources give AL 3 for "Test vehicles" and "Proto events". The ENX handbook for the current VDA ISA catalog is always what counts.

The former labels "Info high" and "Info very high" could only be selected until March 31, 2024. Since then, "Confidential" and "Strictly confidential" apply.

Why EU customers ask for it

Carmakers share design data, software and prototypes with their suppliers long before a model reaches the market. A leak costs them a lot of money. Rather than audit every supplier themselves, they rely on one shared scheme and results that all of them recognize. That is why the required label often appears directly in the supply contract or the tender.

Under [NIS2](#), motor vehicle manufacturers are a regulated sector and have to manage the security of their supply chain. ENX has published an expert opinion showing how far TISAX covers the NIS2 requirements. Personal data, for example from connected vehicles or test drivers, also falls under the [GDPR](#); the "Data" and "Special data" labels exist for this. If you supply connected components, keep the [Cyber Resilience Act](#) in view as well and agree with your customer whether it applies to the part.

Who needs it in South America

- Suppliers to German carmakers in Brazil, for example in the São Paulo area, in Paraná or in Minas Gerais
- Suppliers in Argentina, mainly around Córdoba, Buenos Aires and Rosario
- Engineering and design service providers who work with the manufacturers' CAD data
- Software companies that develop control units, infotainment or backend systems for the auto industry
- Tool and mold makers who see parts before series production starts
- Logistics firms, test tracks and agencies that handle prototypes or test vehicles

Your customer decides which label you need. Ask for the exact label before you register: a label that is too low is useless, and one that is too high costs you time for nothing. If you see prototype parts or prototype vehicles, or receive information with a very high protection need, the table above shows you need an AL 3 label with an on-site audit. Factor that into your timeline and budget.

Steps to the label

1. Register in the ENX portal: enter your company, contact person, locations (assessment scope) and assessment objectives.
2. Complete the self-assessment with the ISA catalog. This is where your gaps show up.
3. Close the gaps: policies, access control, visitor rules, encryption, supplier management and, for prototypes, physical security too.
4. Choose and hire an audit provider approved by ENX.
5. Go through the assessment at the chosen level.
6. If there are findings, submit a corrective action plan and, where needed, go through a follow-up assessment.
7. Receive the assessment report and label and share them with your customers through the ENX portal.

In practice, it often takes several months from registration to label, and more like 6 to 12 months for companies without an existing ISMS. With ISO/IEC 27001 as a starting point, it usually goes faster. All of this depends heavily on the label, the number of locations and where you start, so treat it as a rough guide, not a promise. The ENX fee is listed in the portal; the cost of the audit provider and of preparation varies widely with scope.

Accreditation: what is different with TISAX

TISAX does not run through the classic system of accreditation bodies and certification bodies. Only audit providers approved by ENX may carry out assessments, and ENX oversees them centrally so that results stay comparable. A national accreditation is not enough. ENX publishes the list of approved audit providers on its website; look there for auditors who work in your country and your language.

For ISO/IEC 27001, which you may be pursuing in parallel, the national accreditation bodies do apply: Cgcre at INMETRO in [Brazil](#), OAA in [Argentina](#), INN in [Chile](#), ONAC in [Colombia](#), INACAL in [Peru](#), SAE in [Ecuador](#), OUA in [Uruguay](#), ONA in [Paraguay](#) and DTA-IBMETRO in [Bolivia](#). All nine are listed by the Global Accreditation Cooperation Incorporated (successor to IAF and ILAC since January 1, 2026) as

signatories of its recognition arrangement.

Common mistakes

- The company registers without confirming the required label with the customer and later has to be reassessed.
- The assessment scope leaves out the site where customer data or prototypes are actually handled.
- The self-assessment is filled in too optimistically. At AL 2 and AL 3, the auditor asks for evidence.
- Prototype protection is underestimated. Screening, access control, a photo ban and transport rules have to work in daily practice.
- The result is not shared with the customer in the ENX portal. For the buyer, the label then does not exist.

How Sightadel helps

In [Sightadel](#) you can track the measures from your self-assessment as tasks, with evidence, owners and deadlines. If you already hold ISO/IEC 27001, you reuse the same evidence.

FAQ

Is TISAX a certificate?

No. You receive an assessment report and labels that you share with selected customers through the ENX portal. The result is not public.

Does ISO/IEC 27001 replace TISAX?

No, carmakers require the TISAX label. An existing ISMS under ISO/IEC 27001 does make preparation much easier, though.

How long is a TISAX label valid?

The assessment result is valid for three years. After that, you go through the process again.

Can we use an auditor from our own country?

Only if ENX has approved them as a TISAX audit provider. A national accreditation is not enough.

Which tool helps organize TISAX preparation?

A general GRC tool such as [Sightadel](#) helps with tasks, evidence, document control and supplier assessment. TISAX is not a built-in framework there, so you work through the ISA catalog yourself and use the tool to track the resulting measures.

Sources · Last updated: October 11, 2026

ENX: TISAX: <https://enx.com/en-US/TISAX/>

ENX: TISAX Participant Handbook: <https://www.enx.com/handbook/tisax-participant-handbook.html>

ENX: New TISAX labels for confidentiality and availability: <https://portal.enx.com/en-US/news/new-tisax-labels-for-availability/>

ENX: Expert opinion on NIS2 compliance through TISAX: <https://portal.enx.com/TISAX-NIS2-en.pdf>

Global ACI: recognized accreditation bodies: <https://global-aci.org/en/recognised-abs/>

General information, not legal advice. The official texts are authoritative.

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel walks your team through ISO 27001: templates, tasks, evidence and audit preparation in one place. Built and hosted in Germany, with an optional consultant package.

[See Sightadel →](#)



veyrisk shows what attackers can see of your company from the outside: open services, certificates, known vulnerabilities. You can hand the report to EU customers and auditors.

[See veyrisk →](#)



Valar is a hardware firewall running neonotu software. It protects offices and sites and produces the logs NIS2 and ISO 27001 ask for.

[See Valar →](#)

Sightadel, veyrisk and Valar are products of neonotu GmbH, which operates MercoEU.

Which of these apply to your company?

The free EU Readiness Check shows you by industry and country in 10 minutes.

<https://www.mercoeu.com/en/eu-readiness-check>