GUIDE 2025/2026

TISAX guide for the automotive industry

Information security for suppliers and partners, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is TISAX? 3

1.1 The standard in plain words 3

1.2 Assessment levels AL1, AL2, AL3 3

1.3 TISAX vs. ISO 27001 — where do they differ? 4

1.4 How it sits alongside other rules 4

2 Do you need TISAX? 6

3 The road to the label — seven phases 8

4 What does TISAX cost? 10

5 The ten most common mistakes 12

6 Readiness check: are you ready? 14

7 Glossary 16

8 Your next step 18

1 What is TISAX?

1.1 The standard in plain words

TISAX stands for **Trusted Information Security Assessment Exchange** — the industry standard for information security in the automotive sector. Developed by the German Association of the Automotive Industry (VDA) and administered by the **ENX Association**, it allows the level of IT security to be assessed in a harmonised way along the whole automotive supply chain.

Unlike ISO 27001, TISAX is not a management system standard but an **assessment procedure**: an accredited assessment provider rates your measures, and the result is shared as a label in the central ENX portal. Partners and customers see there that you meet certain protection objectives — without having to run an audit of their own each time.

> **The core idea:** TISAX does not ask “do you want information security?” but “can you show that you meet your OEM customers' requirements — and can you share that proof efficiently?”

The basis is the **VDA ISA catalogue** (Information Security Assessment, currently version 6.0) — a standardised checklist of controls in three areas: information security, prototype protection and data protection. Depending on your protection needs and what the customer requires, the assessment runs at one of three levels.

1.2 Assessment levels AL1, AL2, AL3

AL1	AL2	AL3
Self-assessment (rarely required)	Remote assessment (the standard)	On-site assessment (the highest level)

- **AL1** (assessment level 1): a self-assessment only. In practice OEMs rarely accept it — it is more an entry level or an internal record.
- **AL2**: the assessment provider verifies remotely, by telephone, video and reviewing documents. For normal protection needs.
- **AL3**: an on-site audit. Required where protection needs are high — prototype data and particularly sensitive information.

> **Important:** your OEM customer normally decides the level. For tier-1 suppliers to BMW, Mercedes-Benz, VW, Audi, Porsche or Bosch, AL2 is usually the standard; where prototypes are developed, AL3.

1.3 TISAX vs. ISO 27001 — where do they differ?

Both deal with information security, but with a different focus:

Criterion	TISAX	ISO 27001
Type	An assessment with a label	Management system certification
Focus	The automotive supply chain	Across industries
Catalogue	VDA ISA (~100 controls)	93 controls (Annex A)
Validity	3 years	3 years, with an annual surveillance audit
Scope of use	An OEM requirement, rarely voluntary	Largely voluntary
Basis	Builds on ISO 27001 (~80 % overlap)	A standard in its own right

> **Worth knowing:** if you are certified to ISO 27001 you already meet around 80 % of the TISAX requirements. The extra work lies mainly in prototype protection, where it applies, and in administering the ENX portal and getting the scope right.

1.4 How it sits alongside other rules

Rules	Focus	Relevance in automotive
TISAX	Information security in automotive	Mandatory because the OEM requires it
ISO 27001	An ISMS in general	80 % of the TISAX basis
NIS-2	Critical sectors across the EU	Parts of automotive are in scope (machinery)

Rules	Focus	Relevance in automotive
Automotive SPICE	Automotive software development	Quality, not security
VDA 6.3	Automotive process audit	Quality, not security

2 Do you need TISAX?

TISAX is rarely voluntary. The need almost always comes from a customer — and then the question is less whether than by when, and at which level.

What usually triggers it

- **An OEM asks for it in a tender:** BMW, Mercedes-Benz, VW, Audi, Porsche, Bosch, Continental and many others require TISAX labels from their suppliers.
- **A new contract involving data exchange:** as soon as technical drawings, CAD data or prototype information are involved, a label is usually a precondition.
- **Tier-1 asks tier-2 and tier-3:** the requirements are passed down the chain — small suppliers receive them too.

Which companies are typically affected?

- **OEMs:** yes, but usually with extensive certifications of their own.
- **Tier-1 suppliers:** suppliers of series parts and system integrators. AL2 is the standard.
- **Tier-2 and tier-3:** specialist parts, electronics, software. AL2, or AL3 where the data is critical.
- **Engineering providers:** development, CAD, simulation. Usually AL3, because of the prototype data.
- **IT providers to the industry:** hosting, SaaS, managed services. AL2.
- **Logistics:** AL2, depending on the data involved.

The assessment objectives

TISAX assessments are carried out against assessment objectives. Different requirements apply depending on what data you handle:

Objective	In short	Typical use
Info high	Normal protection needs	Standard information from business partners
Info very high	High protection needs	Particularly sensitive business data

Objective	In short	Typical use
Prototype Protection	Prototype protection	Vehicle development, unreleased models
Data Protection (Art. 28)	Processing under the GDPR	Processing personal data on behalf of another
Data Protection (special category)	Special categories of data	Health and biometric data

A real example: a tier-2 sensor supplier with 80 staff is negotiating a series contract for a new VW model. The tender requires TISAX AL2 with "Info high" and "Prototype Protection" within nine months. No label, no contract.

Planning the timing

OEMs set deadlines, usually six to twelve months to the first assessment. Start too late and you lose the contract. Realistic planning:

- **With ISO 27001 already in place:** four to six months to the label.
- **From scratch:** six to ten months.
- **AL3 with prototype protection:** two months more for the specific measures.

3 The road to the label — seven phases

TISAX follows a structured path. Depending on where you start and which level applies, the whole process takes between **three and ten months**.

1 **Scoping and registering with ENX**

Set the scope: which sites, processes and services go into the assessment? Register on the ENX portal (portal.enx.com) and write the scope description. Two to three weeks.

2 **Gap analysis against the VDA ISA**

Compare your existing measures with the catalogue, identify the gaps and prioritise them by risk. If you have implemented ISO 27001 you will find 80 % already met. Three to four weeks.

3 **Implement the measures**

The real work: implement or improve the controls, write the documentation, adjust the processes. For prototype protection at AL3: physical access control, dedicated networks, encrypted communication. Two to four months.

4 **Self-assessment in the ENX portal**

A structured self-assessment in the portal for every control in the catalogue, with documented answers and evidence. It is the basis for the external assessment. Two to three weeks.

5 **Choose the assessment provider**

Providers accredited by ENX — DEKRA, TÜV, DQS, BSI Group among them. Compare quotations, agree the scope, book the dates. One to two weeks.

6 **The external assessment**

The provider verifies your self-assessment. At AL2 remotely, by telephone, video and document review; at AL3 on site as well. Findings are documented, and you have three months to correct them. One to four weeks.

7 **Publishing the label**

Once the assessment succeeds, the label is published in the portal. You share it with your OEM customers in a click, with no individual audits. It is valid for three years, after which the assessment is repeated. One week.

> **Tip:** Start with an honest gap analysis. Most companies underestimate how deep the documentation has to go. A well-prepared self-assessment cuts the external assessment from three to five days down to one or two.

4 What does TISAX cost?

Cost depends heavily on your size, your scope and the assessment level. Worth knowing: the cost comes in **two parts** — the consulting and build-up, and the external assessment by the provider.

Size of scope	Total cost*	Timeframe	Internal effort
1–20 staff	**€9,900–13,000**	3–5 months	7–12 hrs/week
21–50 staff	**€13,000–18,000**	4–6 months	10–16 hrs/week
51–150 staff	**€16,500–23,000**	5–7 months	12–20 hrs/week
151–500 staff	**€22,000–33,000**	7–10 months	16–26 hrs/week
500+ staff	**€33,000–50,000**	9–14 months	½-1 FTE

* Includes consulting, the gap analysis, implementing the measures and preparing the self-assessment. **The external assessment** by the ENX-accredited provider is billed separately: €5,000–15,000 depending on the level and the scope.

What drives the cost?

- **How many sites are in scope:** each additional site adds 20 to 40 %, and may bring an on-site visit.
- **The assessment level:** AL3 costs around 50 to 80 % more than AL2, because of the on-site audit and the additional physical measures.
- **Prototype protection:** dedicated networks, physical security, managing non-disclosure agreements — all extra work.
- **An existing ISMS (ISO 27001):** cuts the cost by 30 to 50 %.

Costs after the first label

A label is valid for three years, after which the assessment is repeated. In between:

- Maintaining and updating the documentation each year
- The re-assessment in year three, around 60 to 70 % of the original cost
- The ENX portal fee, a small annual contribution

In the interest of transparency: where you need several labels — “Info high” plus “Prototype Protection”, say — each objective adds assessment cost. Combine them from the start to avoid auditing twice.

5 The ten most common mistakes

From guiding a good many TISAX projects, we know the usual stumbling blocks:

1. **Drawing the scope too wide**
   The whole company instead of just the part serving automotive customers. That triples the work for no additional benefit.

2. **Misreading what the OEM requires**
   Commissioning AL2 when the customer asks for AL3. The label is then worthless to that customer.

3. **Underestimating prototype protection**
   Dedicated networks, physical security zones and managing non-disclosure agreements are often planned too late — and they drive cost sharply.

4. **Choosing the provider too late**
   Qualified assessors are scarce, especially at busy times. Booking at least three months ahead is essential.

5. **Filling in the self-assessment sloppily**
   A superficial self-assessment increases the work for the assessor, who then asks more questions and raises more findings.

6. **Documentation nobody lives by**
   Perfect policies that nobody knows about show up immediately in an on-site assessment. Assessors ask the staff directly.

7. **Risk management for form's sake**
   Risk management is the foundation. Filled in without actually treating the risks identified, the assessment has no substance.

8. **No commitment from management**
   Management has to stand behind the assessment visibly — not just with a signature but with resources and attention.

9 **Not fixing findings in time**

After the assessment you have three months to put things right. Miss it and the assessment is repeated — expensive and slow.

10 **Forgetting the re-assessment**

The label is valid for three years. Put the re-assessment off and you risk being without one at short notice — with everything that means for your OEM relationships.

6 Readiness check: are you ready?

The following ten questions let you judge quickly where your company stands on TISAX today:

1. **Do you know the exact scope of your planned assessment?**
   Which sites, processes and services are to be included?
2. **Have you settled which assessment level your customer requires?**
   What the OEM requires sets the bar, and with it the cost and effort.
3. **Do you have ISO 27001 or a comparable ISMS?**
   It cuts the effort by around half, because 80 % of it overlaps.
4. **Is an information security policy documented and actively maintained?**
   The basis of every assessment.
5. **Do you carry out risk analyses regularly?**
   The catalogue requires documented risk management with the risks actually treated.
6. **Is your access management structured and documented?**
   Including a joiner-mover-leaver process and permission reviews.
7. **Do you have an incident response plan with clear reporting routes?**
   Including how you tell OEM customers if data leaks.
8. **Are your staff trained on information security regularly?**
   A mandatory requirement in the catalogue — documented every year.
9. **For AL3 and prototype protection: do you have dedicated physical and logical zones?**
   Access control, encrypted communication, managing non-disclosure agreements.
10. **Have you appointed an information security officer?**
    Internal or external — the catalogue expects clear responsibility.

Your yes answers	Assessment	Recommendation
0–3 × yes	**New ground**	Building up in a structured way, with support, is advisable. Expect six to ten months.
4–6 × yes	**Partly prepared**	Focus on the gaps, above all documentation and risk management. Four to six months.
7–10 × yes	**A good basis**	You can prepare for the assessment in two to four months.

> Whatever your result: **every company can reach TISAX.** It is not a question of size but of preparing in a structured way.

7 Glossary

The key TISAX terms, explained plainly:

TISAX

Trusted Information Security Assessment Exchange — the industry assessment procedure for information security in automotive.

VDA

The German Association of the Automotive Industry — the trade body that publishes the VDA ISA catalogue.

VDA-ISA

VDA Information Security Assessment — the catalogue of around 100 controls. Currently version 6.0.

ENX Association

The administrator of TISAX. It runs the portal and accredits the assessment providers.

ENX-Portal

The central platform (portal.enx.com) for registration, self-assessment and publishing the label.

Assessment Level (AL1, AL2, AL3)

How deep the assessment goes. AL1 is a self-assessment (rare), AL2 is remote, AL3 is on site.

Assessment Objective

An objective such as “Info high”, “Prototype Protection” or “Data Protection” — it determines which controls apply.

Prototype protection

A special category protecting unreleased vehicle information: drawings, CAD data, prototypes.

Label

The result of a successful assessment. Shareable with customers in the portal. Valid for three years.

Assessment provider

A company accredited by ENX — DEKRA, TÜV or DQS, for example — that carries out the assessments.

Scope

What the assessment covers: which sites, systems and processes are included.

OEM

Original equipment manufacturer — BMW, Mercedes-Benz, VW, Audi, Porsche. They typically require TISAX.

Tier-1 / Tier-2 / Tier-3

The supplier hierarchy. Tier-1 supplies the OEM directly, tier-2 supplies tier-1, and so on.

Re-Assessment

A fresh assessment to renew the label once the three years are up.

Nonconformity / Finding

A shortcoming found during the assessment. Three months to put it right, or the assessment is repeated.

8 Your next step

You have read this guide — that is the first step already. Tackling TISAX in a structured way secures your contracts in the automotive industry and positions you as a dependable partner in the supply chain.

A free first conversation

In 30 minutes, with no obligation, we work out together:

- ✓ Which assessment level applies to you?
- ✓ What is the right scope for you?
- ✓ What timeframe and budget are realistic?
- ✓ Which next steps make sense?

No sales pitch, no pressure — just an honest assessment.

> **The quick TISAX check**
> At **iso-easy.de** you will find our free TISAX check. In a few minutes you get a first view of the level, the time and the budget.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

iso-easy.de

iso-easy is part of notivia GmbH.

With more than 30 years of experience in IT consulting and information security we support automotive suppliers in implementing TISAX, ISO 27001 and neighbouring standards — pragmatically, transparently and as equals.

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.