PENTESTERRA

TISAX GAP ASSESSMENT

Would Your TISAX Label Survive an Automotive Tender?

Gap assessment across 41 controls in the Information Security module of VDA ISA 6, for automotive suppliers that need to obtain or maintain a TISAX label.

IN SHORT

Covers the Information Security module (chapters 1-8, ~41 controls) of VDA ISA 6, with the Prototype Protection and Data Protection modules included only where the assessment objective requires them.

41
Information Security module controls

VDA ISA 6
Control numbering aligned to the standard

Automotive
Required by OEMs and Tier 1 suppliers

THE SITUATION TODAY

WHO YOU ARE

You're the security lead of an automotive supplier that needs to obtain or renew a TISAX label to keep working with OEMs and Tier 1 suppliers in the sector.

WHAT HAPPENED

An OEM or Tier 1 requires a TISAX label as a condition to keep supplying, and the assessment with the accredited ENX provider is coming up.

WHY IT HURTS

Without a valid TISAX label, an automotive supplier risks direct exclusion from the supply chain of OEMs and Tier 1s that require it as a contractual condition.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.

THE SOLUTION

Pentesterra's TISAX Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.

WHY IT'S DIFFERENT

You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of TISAX, grouped the way you'll see them in the platform.

Policy, HR, Physical Security (ch. 1-3)

The organizational foundations required by VDA ISA.

- Information security policy
- Human resources security
- Business continuity and physical security

Identity & Access, IT Operations (ch. 4-5)

The day-to-day technical controls.

- Identity and access management
- Operational security of IT infrastructure

Development, Suppliers, Compliance (ch. 6-8)

The software and supply-chain lifecycle.

- Secure system development and acquisition
- Supplier security management
- Regulatory and contractual compliance

Additional modules: Prototype and Data Protection

Included only where the assessment objective requires them.

- Prototype and vehicle protection
- Automotive-specific data protection

PENTESTERRA

TISAX GAP ASSESSMENT

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for TISAX

A complete report, ready to present to clients, auditors, or your board.

Request your TISAX Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance