TISAX® CONSULTANCY

Automotive Industry
Information Security Assessment

WWW.AKRUP.COM

What is TISAX®?

TISAX® (Trusted Information Security Assessment Exchange) enables mutual acceptance of Information Security Assessments in the automotive industry and provides a common assessment and exchange mechanism. TISAX® (VDA ISA) is the German automotive Information Security Assessment.
VDA (Verband der Automobilindustrie) is a German Association of the Automotive Industry. There are more than 600 companies who are members of the VDA. In Germany they manufacture cars, trailers, bodies, and buses as well as parts and accessories, and are represented around the globe. These are not just large corporations; 70% of the added value comes from suppliers, many of whom make up the renowned SMEs of the "German Mittelstand".

The automotive way

While some VDA member companies use the VDA ISA just for internal purposes, others use it to assess the maturity of the information security management of their suppliers. In some of these cases a “self-assessment” was a sufficient basis for the business relationship. For certain cases however, companies conducted a complete assessment of their supplier's information security management (including on-site audits).

If your organization supplies services to one of the VDA-member companies, it is highly likely you would be asked to undergo the TISAX® assessment. This document will provide a high-level overview of the TISAX® process. For any assistance with TISAX® audit, please contact us: info@akrup.com or +44 7801 919154.

Steps to achieve TISAX® label

1. **Registration**. ENX TISAX® will gather information about your company and what needs to be part of the assessment
2. Selection of the **audit provider**
3. **Assessment.** You go through the assessment(s), conducted by one of ENX TISAX®-accredited audit providers
4. **Exchange** You share your assessment result with your partner (who requested the audit)

Registration

To participate in TISAX® process, you need to register with ENX TISAX® Association : https://enx.com/tisax/tisax-en.html#registration

During the online registration process:

- They will ask you for contact details and billing information
- You will have to accept ENX's terms and conditions
- You will have to define the scope of your information security assessment

Audit providers

Currently, there are ten ENX TISAX®-accredited audit providers performing assessments all over the world:

- Ernst & Young GmbH
- KPMG AG
- Operational services GmbH & Co. KG
- PwC Certification Services GmbH
- TÜV Rheinland i-sec GmbH
- DEKRA Certification GmbH
- DQS BIT GmbH
- TÜV NORD CERT GmbH
- Deloitte Certification Services GmbH
- TÜV SÜD Management Service GmbH

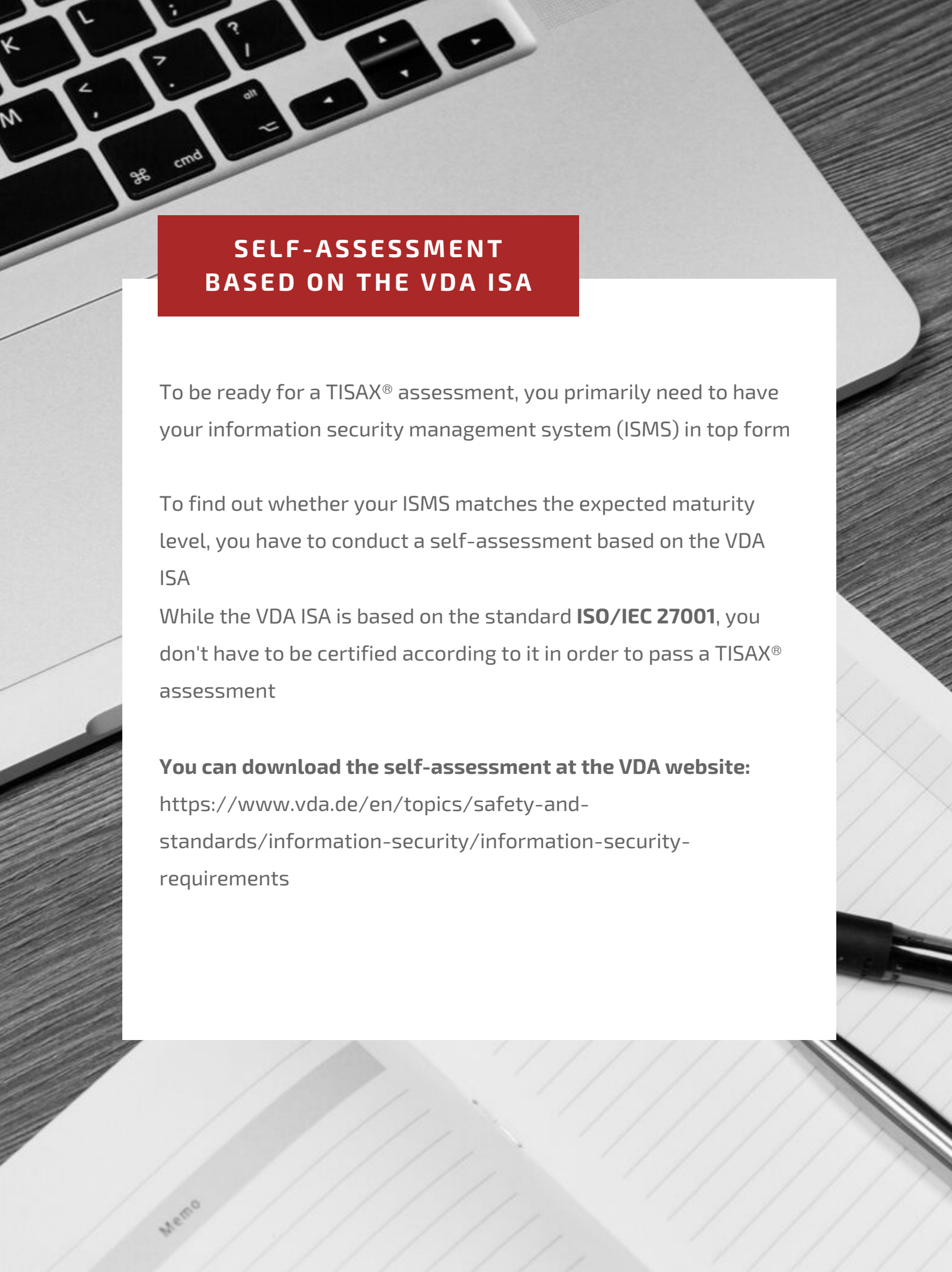
Asessment

There are three levels of TISAX®assessments:

Level 1. Is a self-assessment. Results of assessments with assessment level 1 have a low trust level and are thus not used in TISAX®. But it is of course possible that your partner may request such a self-assessment outside of TISAX®

Level 2. For an assessment with assessment level 2, the audit provider does a plausibility check on your self-assessment (for all locations within assessment scope). He supports this by checking evidences and conducting interviews. Assessments with assessment level 2 generally do not include an on-site inspection

Level 3. For an assessment with assessment level 3, the audit provider does all the checks as for an assessment with assessment level 2. However, all checks will be more comprehensive, and the auditor will thoroughly verify your self-assessment result in an in-depth on-site inspection and interviews in person



SELF-ASSESSMENT BASED ON THE VDA ISA

To be ready for a TISAX® assessment, you primarily need to have your information security management system (ISMS) in top form

To find out whether your ISMS matches the expected maturity level, you have to conduct a self-assessment based on the VDA ISA

While the VDA ISA is based on the standard **ISO/IEC 27001**, you don't have to be certified according to it in order to pass a TISAX® assessment

You can download the self-assessment at the VDA website:
https://www.vda.de/en/topics/safety-and-standards/information-security/information-security-requirements

TISAX® assessment types and elements

The TISAX® assessment process is made up of these three types of TISAX® assessments:

- Initial assessment
- Corrective action plan assessment
- Follow-up assessment

The initial assessment marks the start of the TISAX® assessment process.

The other two TISAX® assessments may take place and may do so several times. They will take place either:

- until you closed all gaps
- or you exit the TISAX® assessment process
- or you reach the maximum time period of nine months (at which point another initial assessment is required)

Audit findings

TISAX® differentiates four types of findings:

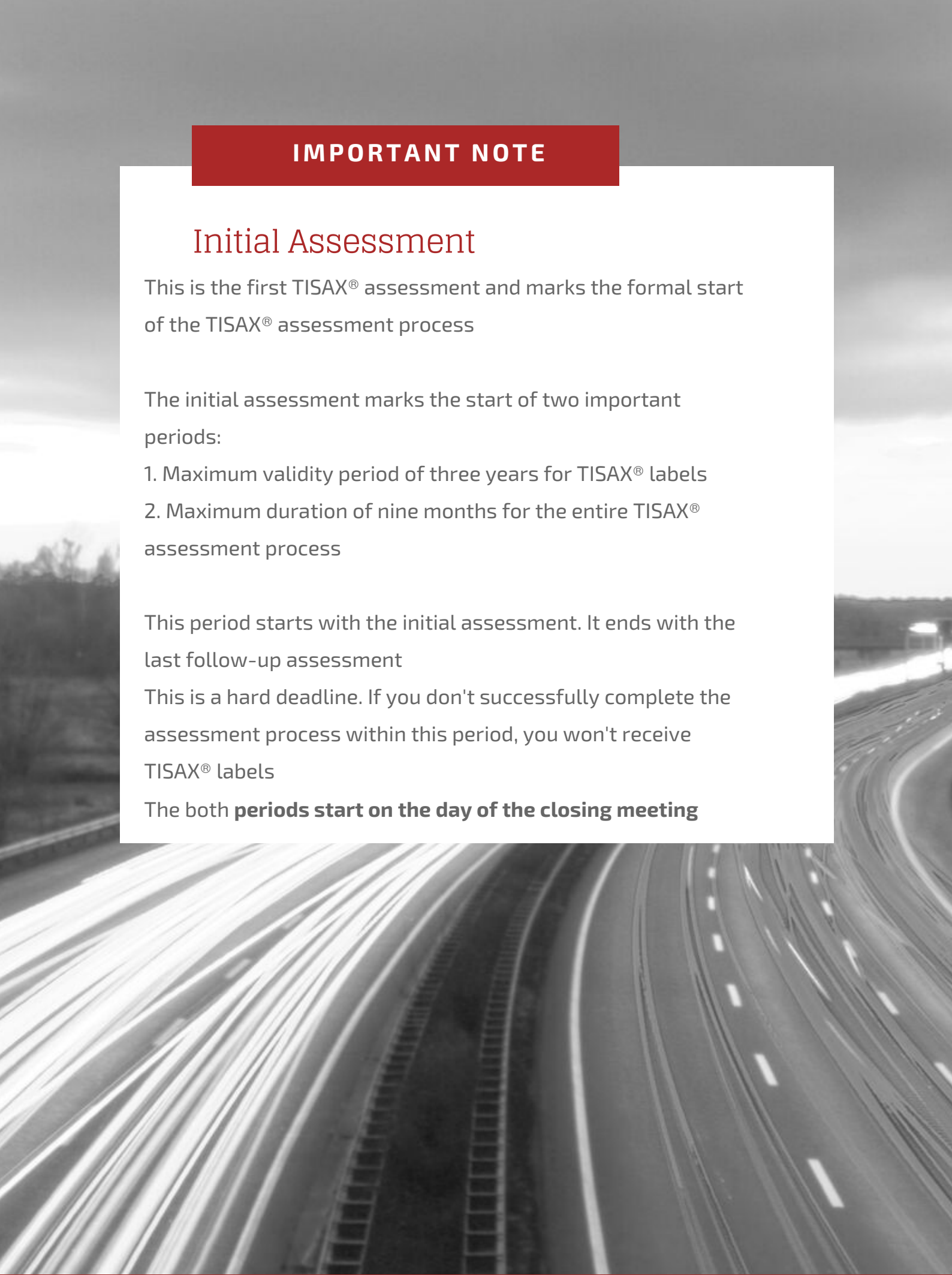
- Observation
- Room for improvement
- Minor non-conformity
- Major non-conformity

Only the two non-conformities are relevant for the assessment result

About conformity

If your overall assessment result is:

- “minor non-conform”, you can receive temporary TISAX® labels until all non-conformities are resolved
- “major non-conform”, you have to resolve the respective issue first before you can receive any TISAX® labels. With appropriate compensating measures and corrective actions approved by the audit provider it is possible to change your overall assessment result from “major non-conform” to “minor non-conform” and thus receive temporary TISAX® labels



IMPORTANT NOTE

Initial Assessment

This is the first TISAX® assessment and marks the formal start of the TISAX® assessment process

The initial assessment marks the start of two important periods:

1. Maximum validity period of three years for TISAX® labels
2. Maximum duration of nine months for the entire TISAX® assessment process

This period starts with the initial assessment. It ends with the last follow-up assessment

This is a hard deadline. If you don't successfully complete the assessment process within this period, you won't receive TISAX® labels

The both **periods start on the day of the closing meeting**

ISO 27001
Protecting your information and reputation

Ensure that sensitive customer and company information is in safe hands with ISO 27001

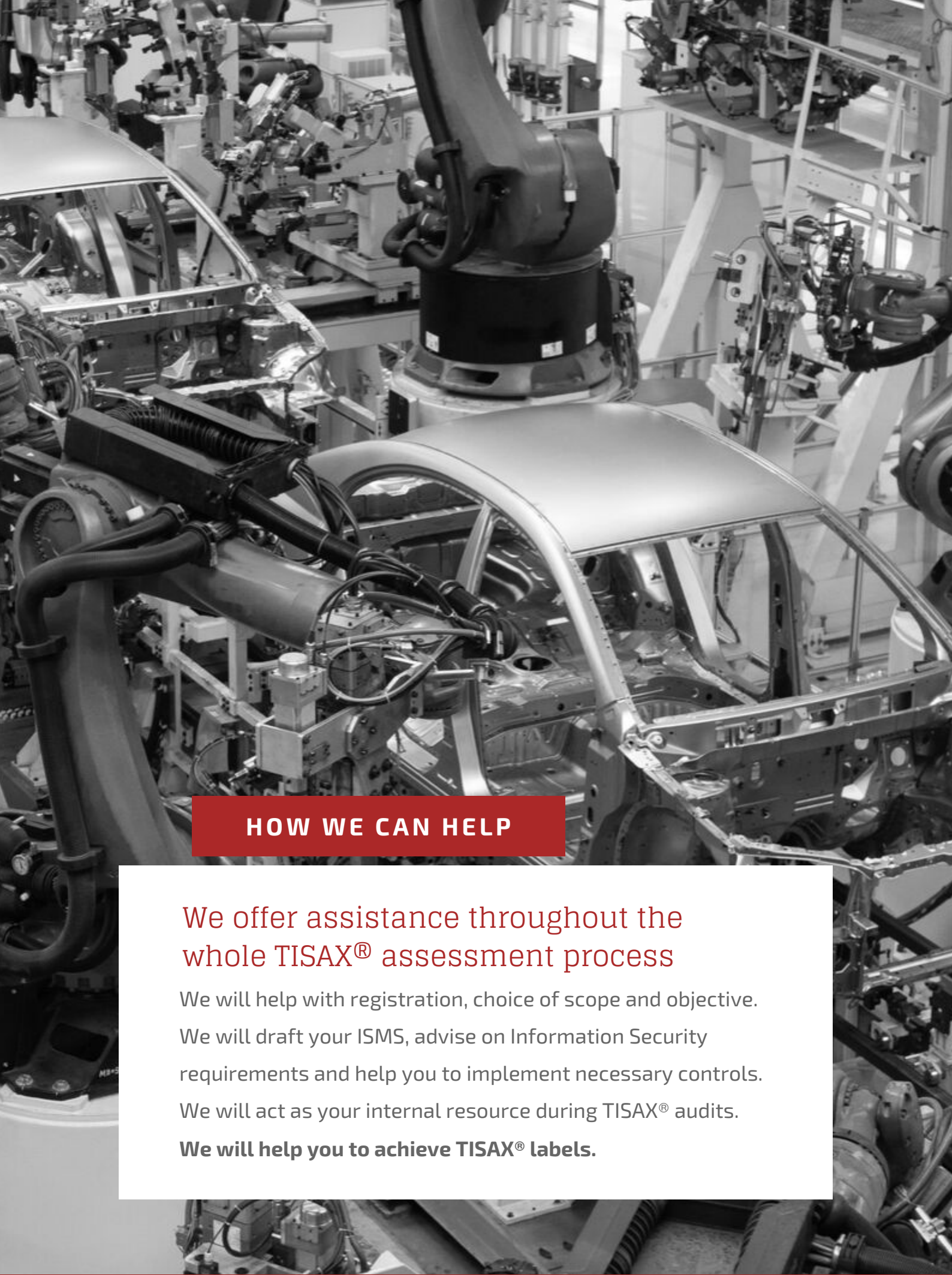
You simply can't be too careful when it comes to protecting personal records and commercially sensitive information

We will help you to implement and maintain a robust and systematic approach to managing information

ISO 27001 helps make businesses more resilient and responsive to threats to information security

By focusing on the key risks to your organization, you can reduce threats and impact

Third party certification can provide additional reassurance to key stakeholders that risks are being managed effectively



HOW WE CAN HELP

We offer assistance throughout the whole TISAX® assessment process

We will help with registration, choice of scope and objective.

We will draft your ISMS, advise on Information Security requirements and help you to implement necessary controls.

We will act as your internal resource during TISAX® audits.

We will help you to achieve TISAX® labels.

'Our business is enabling others to perform better'

Contact us

For a quality, taylor-made and cost effectice service

Phone +44 7801 919154

Email info@akrup.com