Special Conditions for the Performance of TISAX Assessments by TÜV NORD CERT GmbH

TÜV NORD Certification

Table of Contents

Do you have questions about this service description? We will be happy to assist you further.

You can reach us by email info.tncert@tuev-nord.de or personally from Monday to Friday between 7:30 am and 6:00 pm by calling +49 800 – 2457457.

TÜV NORD CERT GmbH

Langemarckstraße 20

45141 Essen

www.tuev-nord-cert.de

1. Evaluation Basis

The Information Security Assessment (ISA) is based on the current audit catalogue of the VDA in each case and the currently valid boundary conditions (such as the participant manual) of the Trusted Information Security Assessment Exchange (TISAX) and the ENX Association.

2. Terms

Active Participant (Auditee) / Participant:
Organisation that must demonstrate the effectiveness of its ISMS with a TISAX label at the request of one of its customers ("passive participant") (also: client) or wants to do this following own strategic decisions.

Passive Participant / Customer:
Organisation that requests its relevant business partners ("active participants") to demonstrate the effectiveness of its ISMS with a corresponding TISAX label.

TISAX Assessment Provider (TISAX AP):
Body approved by ENX to carry out the TISAX assessments (also: contractor).

Simplified Group Assessments (SGA):
Sampling method for the assessment of participant organisations that spread their activities across several locations.

3. Conditions of Participation / Prerequisites

The participant registers on ENX portal to participate in the TISAX procedure.

For this purpose, the participant (active participant) agrees the following with its customers (passive participant):

- the scope of the TISAX Assessment in relation to relevant Assessment Objectives, necessary Protection Level and the associated Assessment Level with the necessary in-Scope Locations

The basis for this coordination is the consideration of all processes, procedures and resources involved at the locations in the scope with which information is processed that is subject to the safety requirements of partners from the automotive industry. This includes the collection, storage and processing of information.

As a result, the participant receives a Participant ID and a Scope ID or the so-called TISAX Scope Excerpt.

The participant provides this TISAX Scope Excerpt to the TISAX AP for its calculation and offer preparation.

In consultation with the participant, the TISAX AP specifies which assessments are to be carried out at which locations from the above-mentioned specifications between participant and customer. This will be done in a kickoff meeting.

The basis for the assessment to be carried out by the TISAX AP is the participant's self-assessment based on the VDA ISA valid for the assessment. The TISAX AP carries out a plausibility check of the participant's self-assessment and on the basis of this plausibility check the further assessment details are determined for assessment level 1, assessment level 2 and assessment level 3.

Assessment Level (AL)	Brief Description	Protection Level
AL1 (by TISAX AP)	Evaluation of the participant's self-assessment concerning compliance with the controls of the VDA ISA catalog and associated evidences.	Normal
AL2 (by TISAX AP)	Plausibility check of the participant's self-assessment; and the assessment of the evidence; and a telephone or online interview with participant's experts (also on site if required).	High
AL3 (by TISAX AP)	Full and detailed check of self-assessment, including the assessment of evidences via audits and on-site expert interviews.	Very high
Use of the multiple location random sampling procedure (SGA) must be applied for and registered with ENX. This requires an intensive pre-assessment of the central ISMS (Exhaustive Precondition Check) according to AL3 and proof of a particular maturity level and effectiveness of the ISMS. In addition to the head office, a representative random sample of locations is assessed, which is determined as follows (for real values, always use the next larger integer): $No_{locations} \leq 10$: $No_{samples} = 2$ $No_{locations} \leq 50$: $No_{samples} = 0.1*(No_{locations} - 10) + 2$ $No_{locations} > 50$: $No_{samples} = 0.05*(No_{locations} - 50) + 6$ The other locations are then subjected to a simplified assessment.		

Note: *According to the ENX rules, no formal recognitions or reductions of TISAX assessment efforts because of existing ISO 27001 certifications are permitted. Combined or integrated TISAX assessments with ISO 27001 audits must be coordinated in advance with the contractor. Simplified Group Assessments and extensions or reductions of these must also be coordinated.*

4. Evaluation Procedure – Services and Obligations of the Contractual Partners (analogous for Assessment Level 2 and 3 in each case)

I. Initial Assessment

After an inquiry, offer and assignment of the TISAX AP (hereinafter referred to as the contractor) by the participant (hereinafter referred to as the client), a formal opening meeting (kick-off meeting) is held in order to specify or confirm the following:

- The Assessment Scope (Assessment Objectives and the in-Scope Locations),
- the relevant VDA ISA catalogues
- the necessary Assessment Prerequisites e.g. Self Assessment of client, Assessment Process incl. Non-Conformity Management,
- the dates/timeline and the participants on both sides: experts of the client and members of the contractor's assessment team.

The kick-off meeting can also take place by telephone or via a web/video/online conference. The Kick-off Meeting marks the beginning of the TISAX procedure.

Subsequently, the client provides the contractor with the necessary documents of its self-assessment.

The contractor evaluates the documentation (self-assessment and corresponding evidences) for completeness and plausibility and prepares on this basis the assessment:

- draws up a content assessment plan based on the document review,
- coordinates the participants of the assessment and
- coordinates the assessment dates and the assessment process as well as the boundary conditions with all people involved.

The actual assessment is then carried out:

a) for Assessment Level 1 (AL1): Only in the event that a Simplified Group Assessment (SGA) involves a self-assessment of a location that is not included in the sample of the SGA assessment, this detailed assessment is replaced by a check for completeness and plausibility.

b) for Assessment Level 2 (AL2), preferably as a telephone or online expert interview on the basis of the completeness and plausibility assessment of the self-assessment carried out by the contractor and the associated evidences from the client.

c) for Assessment Level 3 (AL3), the full assessment of the self-evaluation and the controls of the VDA ISA catalogue for effectiveness, including all corresponding evidence from audits and on-site expert interviews.

d) In Simplified Group Assessments (SGA) an intensive pre-assessment with Assessment Level 3 intensity is carried out of the following in the headquarters:
a) maturity level and the effectiveness of the ISMS
b) the penetration of the other locations and
c) the assessment of the locations in accordance with the agreed Assessment Objectives.
At the same time the locations outside the defined random sample are subjected to a simplified assessment.

e) The contractor prepares records and a preliminary assessment report, which he explains to the contractor during the so-called Closing Meeting. With the date of the Closing Meeting the 9-month period starts, in wihich the TISAX Assessment process has to be finished. After the Closing Meeting, the contractor creates the final assessment report (Initial Assessment Report) and sends it to the client and then reports to ENX.

II. Corrective Action Plan Assessment

If non-conformities exist after completion of the initial assessment, the client must draw up an action plan (Corrective Action Plan) in a with the contractor agreed period to eliminate these non-conformities. At the client's request, the contractor carries out the review and assessment of this action plan during the so-called Corrective Action Plan Assessment, updates the assessment report from the initial assessment and generates the corrective action plan assessment report based on the agreed corrective action plan. The

contractor will send this to the client. The contractor then reports to ENX and, if the results allow, ENX can issue a temporary TISAX label as an interim assessment result.

III. Follow-Up Assessment

If open non-conformities exist after completion of the initial assessment, an action plan to eliminate these non-conformities must be coordinated with the contractor and then implemented. Afterwards at the client's request, the contractor carries out a review and assessment of the successful implementation of the corrective measures by performing a so-called Follow-Up Assessment depending on the type and extent of the non-conformities: on-site, by telephone, web/video/online conference. Thereafter the contractor prepares the final report (Follow-Up Assessment Report) (as an update of the Corrective Action Plan Assessment Report). The contractor will send this to the client. The contractor then reports to ENX and if the results of the follow-up assessment allow it, i.e. if all non-conformities identified in the initial assessment have been effectively remedied, the ENX can issue the final TISAX label as the final assessment result and accordingly be mapped on the TISAX platform of ENX.
The final TISAX label marks the end of the TISAX assessment process.

The client determines at his own discretion who is allowed to view his assessment results on or via the ENX TISAX platform.

5. Further Information

A TISAX procedure must be completed not later than nine months after closing meeting.

For quality assurance purposes, the contractor carries out a quality check of the reports created by an independent person after each assessment process step. Errors or inconsistencies are detected and then corrected / modified accordingly.

6. Obligation to provide information

At the request of a passive participant, the contractor must provide detailed report versions with the requested level of detail in accordance with the rules set by ENX.