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 under 0800 – 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 ISA assessment 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 Information Security Management System (ISMS) with a TISAX label at the request of one of its customers ("passive participant") (also: client).

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 Accredited Audit Provider (XAP):
Body approved by ENX to carry out the TISAX assessments (also: contractor).

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

3. Conditions of Participation / Prerequisites

The participant registers with ENX 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 ISMS and the locations,
- the relevant VDA-ISA assessment catalogues (e.g. information security, third party involvement, prototype protection and data protection),
- the required assessement objectives (VDA-ISA assessment catalogues and required protection level Normal, High or Very High);
  TISAX label and, as applicable, the corresponding target maturity levels.

As a result, the participant receives a Participant ID and a Scope ID.

The participant informs the commissioned XAP of its Participant ID and Scope ID at the latest when placing the order.

In consultation with the participant, the XAP specifies which assessments are to be carried out at which locations from the above-mentioned specifications between participant and customer. While the self-assessment for Protection Level 1 (Normal) is carried out by the participant itself, the assessments for Protection Level 2 (High) or Protection Level 3 (Very High) are to be carried out exclusively by the XAP. The rule here is that a Level 2 or Level 3 assessment requires a previous self-assessment according to Level 1.

Assessment Level (AL)	Brief Description	Protection Level
AL1 (by participant)	Self-assessment for fulfilment of the controls of the VDA ISA catalogue, including evidences, if applicable completed by check of completeness and plausibility by XAP.	Normal
AL2 (by XAP)	Detailed review of the self-assessment and evidences; and a telephone interview with an expert (also on site if required[1]). Condition: AL1 by participant shall be present.	High
AL3 (by XAP)	Full check of the VDA ISA catalogue and self-assessment, and evidence through audits and on-site expert interviews. Condition: AL1 by participant must be present.	Very high
Use of the "Simplified Group Assessment" (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 its particular maturity level and effectiveness. 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 existing ISO 27001 certifications of TISAX assessments 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.*

[1] *Note: Level 2 assessments of locations in countries on the Activation List must be carried out on site.*
The same applies to the assessment of the VDA ISA catalogues Connection to Third Parties and Prototype Protection.

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

I. Initial Assessment

1. After an inquiry, offer and assignment of the XAP (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 (incl. relevant locations),
   - the relevant VDA-ISA assessment catalogues (information security, third party involvement, prototype protection and data protection),
   - the required assessment objectives (VDA-ISA assessment catalogues and required protection level: High or Very High) and, if applicable, the corresponding target maturity levels, and
   - the procedure, the dates 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 conference. The kick-off meeting marks the beginning of the TISAX procedure

   Subsequently, the client provides the contractor with the necessary documents of the self-assessment (Assessment Level 1) and of the information security management system (ISMS).

2. The contractor evaluates the documentation (self-assessment and corresponding evidence) in detail to understand ISMS and its processes and procedures to prepare audit level 2 or 3.

3. The contractor prepares the actual assessment:
   - draws up a content assessment plan based on the document review (risk assessment),
   - coordinates the team involved for the assessment and
   - coordinates the assessment dates and the assessment process as well as the boundary conditions with all people involved.

4. The actual assessment is then carried out:

   4.0 AL1: Only in the case of reviewing self-assessments of a site not being included in the sample in a SGA assessment, the detailed evaluation (clause 2) is replaced by checking completeness and plausibility only (Assessment Level 1).

   4.1 AL2: For Assessment Level 2, preferably as a telephone expert interview on results of self-assessment and the respective evidence (optionally also as a web or video conference or on-site (in any case with countries of the activation list, connection to third parties and prototype protection)),

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

   4.3 In Simplified Group Assessments an intensive pre-assessment at Level 3 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.

5. The contractor prepares and records a preliminary assessment report, which he subsequently explains to the client ("Closing Meeting"). Closing Meeting defines the beginning of 9-months term where process shall be completed within.
   As a matter of principle, the client has the opportunity to remedy any weaknesses by means of appropriate evidence or action plans (Corrective Action Plans) during the initial assessment, so that additional expenses can be reduced or even avoided.

II. Corrective Action Plan Assessment

If open non-conformities exist after completion of the initial assessment, the client must draw up action plans (Corrective Action Plans) to eliminate these non-conformities within the deadlines specified by ENX.

At the client's request, the contractor carries out the review and assessment of these action plans (Corrective Action Plan Assessment), and

- updates the assessment report from the initial assessment (Update) and
- explains the results and the report to the client in a final meeting.

If enabled by assessment results, contractor will forward the assessment results to ENX to enable issuance of a temporary label.

III. Follow-Up Assessment

If open non-conformities exist after completion of the initial assessment, the client must have implemented effective measures to eliminate these non-conformities (implementation / follow-up) within the periods specified by ENX.

At the client's request, the contractor carries out a review and assessment of the implementation of the corrective measures (follow-up assessment, depending on the type and extent of the non-conformities: on-site, by telephone, web/video conference);

- prepares the final report (as an update of the present version) and
- explains the results and the report to the client in a final meeting.

The contractor forwards the final file to the TISAX platform, where the client releases it at his discretion. The corresponding TISAX labels will be issued by ENX.
This decision marks the end of the TISAX procedure.

5. Further Information

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

For quality assurance purposes, the contractor carries out a so-called veto check after each step, in which the reports and documents that have been draw up are checked for errors or inconsistencies by an independent person and corrected/modified, as necessary.

Contractor may modify these Special Conditions at any time to ensure fulfilling continuously all applicable requirements of ENX as well after modifications. The client shall not disagree these modifications but may use a special right of cancellation to terminate the assessment process.

6. Duty of Disclosure

On request of a passive participant contractor shall provide detailed reports in requested depth of detail according to rules defined by ENX.