

<p>Table of contents</p> <p>1 EVALUATION BASIS</p> <p>2 TERMS</p> <p>3 CONDITIONS OF PARTICIPATION / PREREQUISITES</p> <p>4 EVALUATION PROCEDURE – SERVICES OBLIGATIONS OF THE CONTRACTUAL PARTNERS (ANALOGOUS FOR ASSESSMENT LEVEL 2 AND LEVEL 3 IN EACH CASE)</p> <p style="padding-left: 20px;">I. Initial Assessment</p> <p style="padding-left: 20px;">II. Corrective Action Plan Assessment</p> <p style="padding-left: 20px;">III. Follow-up Assessment</p> <p>5 FURTHER INFORMATION</p> <p>6 OBLIGATION TO PROVIDE INFORMATION</p> <p>Do you have questions about this service description? We will be happy to assist you further.</p> <p>You can reach us by email at info.tncert@tuev-nord.de or personally from Monday to Friday between 7:30 am and 6:00 pm by calling +49 800 – 2457457.</p> <p>TÜV NORD CERT GmbH</p> <p>Langemarckstraße 20</p> <p>45141 Essen</p> <p>www.tuev-nord-cert.de</p>	<p>Tabla de contenido</p> <p>1 BASE DE EVALUACIÓN</p> <p>2 TÉRMINOS</p> <p>3 CONDICIONES DE PARTICIPACIÓN / REQUISITOS PREVIOS</p> <p>4 PROCEDIMIENTO DE EVALUACIÓN - OBLIGACIONES DE SERVICIOS DE LOS SOCIOS CONTRACTUALES (ANÁLOGO PARA EVALUACIÓN NIVEL 2 Y NIVEL 3 EN CADA CASO)</p> <p style="padding-left: 20px;">I. Evaluación inicial</p> <p style="padding-left: 20px;">II. Evaluación del plan de acción correctiva</p> <p style="padding-left: 20px;">III. Evaluación de seguimiento</p> <p>5 MÁS INFORMACIÓN</p> <p>6 OBLIGACIÓN DE SUMINISTRAR INFORMACIÓN</p> <p>¿Tiene preguntas sobre esta descripción de servicio? Estaremos encantados de ayudarle.</p> <p>Puede comunicarse con nosotros por correo electrónico info.tncert@tuev-nord.de o personalmente de lunes a viernes entre las 7:30 am y las 6:00 pm llamando al +49800 - 2457457.</p> <p>TÜV NORD CERT GmbH</p> <p>Langemarckstrasse 20</p> <p>45141 Essen</p> <p>www.tuev-nord-cert.de</p>
--	--

<p>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.</p> <p>2. Terms Active Participant (Auditee) / Participant: The organization 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 its own strategic decisions.</p> <p>Passive Participant / Customer: The organization requests its relevant business partners ("active participants") to demonstrate the effectiveness of its ISMS with a corresponding TISAX label.</p> <p>TISAX Assessment Provider (TISAX AP): The body approved by ENX to carry out the TISAX assessments (also: contractor).</p> <p>Simplified Group Assessments (SGA): Sampling method for the assessment of participant organizations that spread their activities across several locations.</p> <p>3. Conditions of Participation / Prerequisites The participant registers on the ENX portal to participate in the TISAX procedure. For this purpose, the participant (active participant) agrees with the following with its customers (passive participant):</p> <ul style="list-style-type: none"> ▪ 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 <p>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 the participant and customer. This will be done in a kickoff meeting.</p>	<p>1. Base de evaluación La Evaluación de Seguridad de la Información (ISA) se basa en el catálogo de auditoría actual del VDA en cada caso y las condiciones límite actualmente válidas (como el manual del participante) del Trusted Information Security Assessment Exchange (TISAX) y la Asociación ENX.</p> <p>2. Términos Participante activo (auditado) / Participante: Organización que debe demostrar la efectividad de su SGSI con etiqueta TISAX a solicitud de uno de sus clientes ("participante pasivo") (también: cliente) o quiere hacerlo siguiendo sus propias decisiones estratégicas.</p> <p>Participante pasivo / cliente: Organización que solicita a sus socios comerciales relevantes ("participantes activos") que demuestren la efectividad de su SGSI con la etiqueta TISAX correspondiente.</p> <p>Proveedor de evaluación TISAX (TISAX AP): Organismo homologado por ENX para realizar las evaluaciones TISAX (también: contratista).</p> <p>Evaluaciones grupales simplificadas (SGA): Método de muestreo para la evaluación de las organizaciones participantes que distribuyen sus actividades en varios lugares.</p> <p>3. Condiciones de participación / requisitos previos El participante se registra en el portal ENX para participar en el procedimiento TISAX. A tal efecto, el participante (participante activo) acuerda con sus clientes (participante pasivo) lo siguiente:</p> <ul style="list-style-type: none"> ▪ el alcance de la evaluación TISAX en relación con los objetivos de evaluación relevantes, el nivel de protección necesario y el nivel de evaluación asociado con las ubicaciones necesarias dentro del alcance. <p>La base de esta coordinación es la consideración de todos los procesos, procedimientos y recursos involucrados en las ubicaciones en el alcance con el que se procesa la información que está sujeta a los requisitos de seguridad de los socios de la industria automotriz. Esto incluye la recopilación, el almacenamiento y el procesamiento de información. Como resultado, el participante recibe una identificación de participante y una identificación de alcance o el llamado extracto de alcance de TISAX. El participante proporciona este Extracto del Alcance TISAX al TISAX AP para su cálculo y preparación de la oferta.</p>
---	---

<p>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.</p>	<p>En consulta con el participante, el TISAX AP especifica qué evaluaciones se llevarán a cabo en qué ubicaciones de las especificaciones antes mencionadas entre el participante y el cliente. Esto se hará en una reunión inicial.</p> <p>La base de la evaluación a realizar por el TISAX AP es la autoevaluación del participante en base al VDA ISA válido para la evaluación. El TISAX AP lleva a cabo una verificación de plausibilidad de la autoevaluación del participante y, sobre la base de esta verificación de plausibilidad, se determinan los detalles de evaluación adicionales para el nivel de evaluación 1, el nivel de evaluación 2 y el nivel de evaluación 3.</p>
---	---

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 catalogue and associated pieces of evidence.	Normal
AL2 (by TISAX AP)	Plausibility check of the participant's self-assessment; 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 evidence 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.

Nivel de Evaluación (AL)	Breve Descripción	Nivel de Protección
AL1 (por TISAX AP)	Evaluación de la autoevaluación del participante sobre el cumplimiento de los controles del catálogo VDA ISA y evidencias asociadas.	Normal
AL2 (por TISAX AP)	Verificación de plausibilidad de la autoevaluación del participante; y la valoración de la evidencia; y una entrevista telefónica o en línea con los expertos de los participantes (también en sitio si es necesario).	Alto

AL3 (por TISAX AP)	Verificación completa y detallada de la autoevaluación, incluida la evaluación de evidencias mediante auditorías y entrevistas a expertos en sitio.	Muy Alto
<p>El uso del procedimiento de muestreo aleatorio de ubicaciones múltiples (SGA) debe solicitarse y registrarse con ENX. Esto requiere una evaluación previa intensiva del SGSI central (Control exhaustivo de condiciones previas) de acuerdo con AL3 y una prueba de un nivel de madurez y eficacia particulares del SGSI. Además de la oficina central, se evalúa una muestra aleatoria representativa de ubicaciones, que se determina de la siguiente manera (para valores reales, utilice siempre el siguiente entero mayor):</p> <p>$No_{ubicaciones} \leq 10: No_{muestras} = 2$</p> <p>$No_{ubicaciones} \leq 50: No_{muestras} = 0.1 * (No_{ubicaciones} - 10) + 2$</p> <p>$No_{ubicaciones} > 50: No_{muestras} = 0.05 * (No_{ubicaciones} - 50) + 6$</p> <p>Las otras ubicaciones se someten a una evaluación simplificada.</p> <p>Nota: De acuerdo con las reglas de ENX, no se permiten reconocimientos o reducciones formales de los esfuerzos de evaluación de TISAX debido a las certificaciones ISO 27001 existentes. Las evaluaciones TISAX combinadas o integradas con auditorías ISO 27001 deben coordinarse de antemano con el contratista. Las evaluaciones grupales simplificadas y las ampliaciones o reducciones de las mismas también deben coordinarse.</p>		

<p>4. Evaluation Procedure – Services and Obligations of the Contractual Partners (analogous for Assessment Level 2 and 3 in each case)</p> <p>I. Initial Assessment</p> <p>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:</p> <ul style="list-style-type: none"> ▪ 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. <p>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 for its self-assessment.</p> <p>The contractor evaluates the documentation (self-assessment and corresponding evidence) for completeness and plausibility and prepares on this basis assessment:</p> <ul style="list-style-type: none"> ▪ draws up a content assessment plan based on the document review, ▪ coordinates the participants of the assessment and 	<p>4. Procedimiento de evaluación - Servicios y obligaciones de los socios contractuales (análogo para los niveles de evaluación 2 y 3 en cada caso)</p> <p>I. Evaluación Inicial</p> <p>Después de una consulta, oferta y cesión del TISAX AP (en adelante, el contratista) por parte del participante (en adelante, el cliente), se lleva a cabo una reunión formal de apertura (reunión inicial) para especificar o confirmar el siguiente:</p> <ul style="list-style-type: none"> ▪ El alcance de la evaluación (objetivos de la evaluación y las ubicaciones dentro del alcance), ▪ los catálogos VDA ISA relevantes ▪ los requisitos previos necesarios para la evaluación, p. ej. Autoevaluación del cliente, proceso de evaluación incluida la gestión de no conformidades, ▪ las fechas / cronograma y los participantes de ambos lados: expertos del cliente y miembros del equipo de evaluación del contratista. <p>La reunión inicial también puede tener lugar por teléfono o mediante una conferencia web / video / en línea. La reunión de lanzamiento marca el comienzo del procedimiento TISAX. Posteriormente, el cliente proporciona al contratista los documentos necesarios de su autoevaluación.</p> <p>El contratista evalúa la documentación (autoevaluación y las evidencias correspondientes) para verificar que esté completa y sea plausible y prepara sobre esta base la evaluación:</p> <ul style="list-style-type: none"> ▪ elabora un plan de evaluación de contenido basado en la revisión de documentos,
---	---

- 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 pieces of evidence 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 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 which 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) 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

- coordina a los participantes de la evaluación y
- coordina las fechas de evaluación y el proceso de evaluación, así como las condiciones de los límites con todas las personas involucradas.

A continuación, se lleva a cabo la evaluación real:

- a) para el nivel de evaluación 1 (AL1): solo en el caso de que una evaluación de grupo simplificada (SGA) implique una autoevaluación de una ubicación que no esté incluida en la muestra de la evaluación SGA, esta evaluación detallada se sustituye por una verificación para que esté completo y sea plausible.
- b) para el Nivel de Evaluación 2 (AL2), preferiblemente como entrevista telefónica o en línea a un experto sobre la base de la evaluación de la integridad y plausibilidad de la autoevaluación realizada por el contratista y las evidencias asociadas del cliente.
- c) para el Nivel de Evaluación 3 (AL3), la evaluación completa de la autoevaluación y los controles del catálogo de VDA ISA para la efectividad, incluida toda la evidencia correspondiente de auditorías y entrevistas con expertos in situ.
- d) En las Evaluaciones de Grupo Simplificadas (SGA) se realiza una pre evaluación intensiva con intensidad de Nivel de Evaluación 3 de lo siguiente en la sede:
 - a) Nivel de madurez y eficacia del SGSI
 - b) la penetración de los otros lugares y
 - c) la evaluación de las ubicaciones de acuerdo con los objetivos de evaluación acordados. Al mismo tiempo, las ubicaciones fuera de la muestra aleatoria definida se someten a una evaluación simplificada.
 - e) El contratista elabora actas y un informe de evaluación preliminar, que explica al contratista durante la denominada Reunión de Clausura. Con la fecha de la Reunión de Clausura se inicia el plazo de 9 meses en el que se debe finalizar el proceso de Evaluación TISAX. Después de la reunión de cierre, el contratista crea el informe de evaluación final (Informe de evaluación inicial) y lo envía al cliente y luego informa a ENX.

II. Evaluación del Plan de acción correctiva

Si existen no conformidades después de la finalización de la evaluación inicial, el cliente debe elaborar un plan de acción (Plan de Acción Correctiva) en un período acordado con el contratista para eliminar estas no conformidades. A petición del cliente, el contratista lleva a cabo la revisión y evaluación de este plan de acción durante la denominada Evaluación del plan de acción

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 the 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.

correctiva, actualiza el informe de evaluación de la evaluación inicial y genera el informe de evaluación del plan de acción correctiva basado en el plan de acción correctivo acordado. . El contratista enviará esto al cliente. Luego, el contratista informa a ENX y, si los resultados lo permiten, ENX puede emitir una etiqueta TISAX temporal como resultado de la evaluación intermedia.

III. Evaluación de seguimiento

Si existen no conformidades abiertas después de la finalización de la evaluación inicial, un plan de acción para eliminar estas no conformidades debe coordinarse con el contratista y luego implementarse. Posteriormente, a solicitud del cliente, el contratista lleva a cabo una revisión y evaluación de la implementación exitosa de las medidas correctivas mediante la realización de la denominada Evaluación de Seguimiento en función del tipo y alcance de las no conformidades: in situ, por teléfono , conferencia web / video / online. Posteriormente, el contratista prepara el informe final (Informe de evaluación de seguimiento) (como una actualización del Informe de evaluación del plan de acción correctiva). El contratista enviará esto al cliente. Luego, el contratista informa a ENX y si los resultados de la evaluación de seguimiento lo permiten, es decir, Si todas las no conformidades identificadas en la evaluación inicial se han solucionado de manera efectiva, ENX puede emitir la etiqueta TISAX final como resultado de la evaluación final y, en consecuencia, ser mapeada en la plataforma TISAX de ENX. La etiqueta final de TISAX marca el final del proceso de evaluación de TISAX. El cliente determina a su propia discreción quién puede ver los resultados de su evaluación en la plataforma ENX TISAX o a través de ella.

5. Más información

Un procedimiento TISAX debe completarse a más tardar nueve meses después de la reunión de cierre. Para fines de garantía de calidad, el contratista lleva a cabo un control de calidad de los informes creados por una persona independiente después de cada paso del proceso de evaluación. Los errores o inconsistencias se detectan y luego se corrigen / modifican en consecuencia.

6. Obligación de proveer información

A solicitud de un participante pasivo, el contratista debe proporcionar versiones detalladas del informe con el nivel de detalle solicitado de acuerdo con las reglas establecidas por ENX.

