

Special Conditions for the Performance of TISAX® Assessments by TÜV NORD CERT GmbH / Condiciones Especiales para la realización de Assessments de TISAX® por TÜV NORD CERT GmbH

Table of contents	Tabla de contenidos
<ol style="list-style-type: none"> 1. EVALUATION BASIS 2. TERMS 3. CONDITIONS OF PARTICIPATION / PREREQUISITES 4. EVALUATION PROCEDURE – SERVICES AND OBLIGATIONS OF THE CONTRACTUAL PARTNERS (ANALOGOUS FOR ASSESSMENT LEVEL 2 AND 3 IN EACH CASE) 	<ol style="list-style-type: none"> 1. BASES DE LA EVALUACIÓN 2. TÉRMINOS 3. CONDICIONES DE PARTICIPACIÓN / PRE-REQUISITOS 4. PROCEDIMIENTO DE EVALUACIÓN – SERVICIOS Y OBLIGACIONES DE LAS PARTES CONTRATANTES (ANÁLOGO PARA LOS NIVELES DE EVALUACIÓN 2 Y 3 EN CADA CASO)
<ol style="list-style-type: none"> I. Initial Assessment II. Corrective Action Plan Assessment III. Follow-Up Assessment 	<ol style="list-style-type: none"> I. Initial Assessment II. Corrective Action Plan Assessment III. Follow-Up Assessment
<ol style="list-style-type: none"> 5. FURTHER INFORMATION 6. OBLIGATION TO PROVIDE INFORMATION 	<ol style="list-style-type: none"> 5. INFORMACIÓN ADICIONAL 6. OBLIGACIÓN DE PROPORCIONAR INFORMACIÓN
<p>Do you have questions about this service description? We will be happy to assist you further.</p>	<p>¿Tiene alguna pregunta sobre la descripción de este servicio? Estaremos encantados de ayudarle.</p>
<p>You can reach us by email info.cert@tuev-nord.de or personally from Monday to Friday between 7:30 am and 6:00 pm by calling +49 800-2457457</p>	<p>Puede ponerse en contacto con nosotros por correo electrónico info.cert@tuev-nord.de o personalmente de lunes a viernes entre las 7.30 y las 18.00 horas llamando al +49 800-2457457.</p>
<p>TÜV NORD CERT GmbH Am TÜV 1 45307, Essen</p>	<p>TÜV NORD CERT GmbH Am TÜV 1 45307, Essen</p>

1. Evaluation Basis

The Information Security Assessment (ISA) is based on the current audit catalogue ISA 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: Organization 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:

Organization 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 organizations that have spread their activities across several locations and want to have those audited in one assessment.

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 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

1. Evaluation Basis

La evaluación de la seguridad de la información (ISA) se basa en el catálogo de auditoría ISA vigente de la VDA en cada caso y en las condiciones límite actualmente vigentes (como el manual del participante) del Trusted Information Security Assessment Exchange (TISAX®) y de la Asociación ENX.

2. Términos

Participante activo (auditado) / Participante:

Organización que debe demostrar la eficacia de su SGSI con una etiqueta TISAX® a petición de uno de sus clientes ("participante pasivo") (también: cliente) o quiere hacerlo a raíz de decisiones estratégicas propias.

Participante pasivo / Cliente:

Organización que solicita a sus socios comerciales relevantes ("participantes activos") que demuestren la eficacia de su SGSI con la correspondiente etiqueta TISAX®.

Proveedor de Evaluación TISAX® (PA TISAX®):

Organismo autorizado por ENX para realizar las evaluaciones TISAX® (también: contratista).

Evaluaciones de grupo simplificadas (SGA):

Método de muestreo para la evaluación de organizaciones participantes que tienen repartidas sus actividades en varias ubicaciones y desean que éstas sean auditadas en una sola evaluación.

3. Condiciones de participación / Requisitos previos

El participante se registra en el portal de ENX para participar en el procedimiento TISAX®.

Para ello, el participante (participante activo) acuerda lo siguiente con sus clientes (participante pasivo):

- El alcance de Evaluación TISAX® en relación con los Objetivos de Evaluación pertinentes y el Nivel de Evaluación asociado con las ubicaciones in-Scope necesarias.

La base de esta coordinación es la consideración de todos los procesos, procedimientos y recursos

business partners. 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 kick-off 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 catalogue and associated evidences. This is only relevant for Simplified Group Assessments.	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 (Nosamples) out of all locations in the scope (Nolocations) is assessed, which is determined as follows (for real values, always use the next larger integer):

implicados en los lugares del ámbito con los que se procesa información sujeta a los requisitos de seguridad de los socios comerciales. Esto incluye la recogida, el almacenamiento y el tratamiento de la información.

Como resultado, el participante recibe un Participant-ID y un Scope-ID o el llamado TISAX® Scope Excerpt.

El participante proporciona este TISAX® Scope Excerpt al TISAX® AP para su cálculo y preparación de la oferta.

En consulta con el participante, el TISAX® AP especifica qué evaluaciones deben realizarse y en qué lugares a partir de las especificaciones mencionadas entre el participante y el cliente. Esto se hará en una reunión inicial (kick-off meeting).

La base de la evaluación que llevará a cabo el TISAX® AP es la autoevaluación del participante basada en el VDA ISA válido para la evaluación. El PA de TISAX® llevará a cabo un control de plausibilidad de la autoevaluación del participante y, sobre la base de este control de plausibilidad, se determinarán los demás detalles de la evaluación para el nivel de evaluación 1, el nivel de evaluación 2 y el nivel de evaluación 3.

Nivel de Assessment (AL)	Descripción Breve	Nivel de protección
AL1 (by TISAX® AP)	Evaluación de la autoevaluación del participante en relación con el cumplimiento de los controles del catálogo VDA ISA y las pruebas asociadas. Esto sólo es pertinente para las evaluaciones de grupo simplificadas	Normal
AL2 (by TISAX® AP)	Comprobación de la plausibilidad de la autoevaluación del participante y de la evaluación de las pruebas, y entrevista telefónica o en línea con los expertos del participante (también en sitio si es necesario).	Alta
AL3 (by TISAX® AP)	Comprobación completa y detallada de la autoevaluación, incluida la	Muy Alta

<p>Nosamples(Nolocations) = $\lceil \sqrt{Nolocations} \rceil$</p> <p>The other locations are then subjected to a simplified assessment.</p>	<p>evaluación de las pruebas mediante auditorías y entrevistas a expertos en sitio.</p>
<p>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.</p> <p><i>Simplified Group Assessments and extensions or reductions of these must also be coordinated.</i></p> <p><i>Assessments following AL2,5 have to be coordinated as well in advance with the contractor.</i></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. (Only those dates and timelines are binding!) <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.</p> <p>Subsequently, the client provides the contractor with the necessary documents of its self-assessment.</p>	<p>El uso del procedimiento de muestreo aleatorio de ubicaciones múltiples (SGA) debe solicitarse y registrarse en ENX. Para ello se requiere una preevaluación intensiva del SGSI central (Exhaustive Precondition Check) de acuerdo con AL3 y la prueba de un determinado nivel de madurez y eficacia del SGSI. Además de la sede central, se evalúa una muestra aleatoria representativa (Nosamples) de todas las ubicaciones del alcance (Nolocations), que se determina de la siguiente manera (para valores reales, utilice siempre el siguiente número entero mayor):</p> <p>Nosamples(Nolocations) = $\lceil \sqrt{Nolocations} \rceil$</p> <p>Los demás lugares se someten a una evaluación simplificada.</p> <p>Nota: De acuerdo con las normas ENX, no se permiten reconocimientos formales ni reducciones de los esfuerzos de evaluación TISAX® debido a certificaciones ISO 27001 existentes. Las evaluaciones TISAX® combinadas o integradas con auditorías ISO 27001 deben coordinarse previamente con el contratista.</p> <p><i>También deben coordinarse las evaluaciones de grupo simplificadas y sus ampliaciones o reducciones.</i></p> <p><i>Las evaluaciones según AL2,5 también deben coordinarse previamente con el contratista.</i></p> <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. Initial Assessment</p> <p>Tras la consulta, oferta y asignación del TISAX® AP (en lo sucesivo, el contratista) por parte del participante (en lo sucesivo, el cliente), se celebra una reunión formal de apertura (kick-off meeting) con el fin de especificar o confirmar lo siguiente:</p> <ul style="list-style-type: none"> ▪ El alcance de la evaluación (los objetivos de la evaluación y las ubicaciones dentro del alcance), ▪ los catálogos VDA ISA pertinentes ▪ los requisitos previos necesarios para la evaluación, como la autoevaluación del cliente

<p>The contractor evaluates the documentation (self-assessment and corresponding evidences) for completeness and plausibility and prepares on this basis the 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 ▪ coordinates the assessment dates and the assessment process as well as the boundary conditions with all people involved. <p>The actual assessment is then carried out:</p> <p>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 and the assessment objective requires an AL2 audit, this detailed assessment is replaced by a simple check for completeness and plausibility.</p> <p>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.</p> <p>c) for Assessment Level 3 (AL3): 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.</p> <p>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 Additionally the assessment of the sample locations (Nosamples) in accordance with the agreed Assessment Objectives has to be performed. At the same time the locations outside the defined random sample are subjected to a simplified assessment.</p> <p>e) The contractor prepares records and a preliminary assessment report, which he explains to the contractor during the so-called Closing Meeting.</p>	<p>o el proceso de evaluación, incluida la gestión de no conformidades,</p> <ul style="list-style-type: none"> ▪ las fechas/plazos y los participantes de ambas partes: expertos del cliente y miembros del equipo de evaluación del contratista. (Sólo estas fechas y plazos son vinculantes). <p>La reunión inicial también puede celebrarse por teléfono o a través de una conferencia web/vídeo/online. La reunión inicial marca el inicio del procedimiento TISAX®.</p> <p>Posteriormente, el cliente facilita al contratista los documentos necesarios de su autoevaluación</p> <p>El contratista evalúa la documentación (autoevaluación y pruebas correspondientes) para comprobar si está completa y es plausible y prepara sobre esta base la evaluación:</p> <ul style="list-style-type: none"> ▪ elabora un plan de evaluación del contenido basado en la revisión de la documentación, ▪ coordina a los participantes en la evaluación y ▪ coordina con todas las personas implicadas las fechas y el proceso de evaluación, así como las condiciones límite. <p>Posterior a esto se lleva a cabo el Assessment:</p> <p>a) para el Assessment Nivel 1 (AL1): Sólo en el caso de que una Evaluación Simplificada de Grupo (SGA) implique una autoevaluación de un lugar que no esté incluido en la muestra de la evaluación SGA y el objetivo de la evaluación requiera una auditoría AL2, esta evaluación detallada se sustituye por una simple comprobación de integridad y verosimilitud.</p> <p>b) para el Assessment Nivel 2 (AL2): Preferiblemente en forma de entrevista telefónica o en línea con un experto sobre la base de la evaluación de la exhaustividad y la verosimilitud de la autoevaluación realizada por el contratista y las pruebas asociadas del cliente.</p> <p>c) Para el Assessment Nivel 3 (AL3): Evaluación completa de la eficacia de la autoevaluación y los controles del catálogo ISA de VDA, incluidas todas las pruebas correspondientes de auditorías y entrevistas a expertos en sitio.</p>
---	--

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. In case the results enable it and no nonconformities have been identified, a TISAX® label can be issued by 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.

- d) En los Assessments de Grupo Simplificados (SGA) se lleva a cabo una preevaluación intensiva de Nivel de Evaluación 3 de los siguientes aspectos en la sede central: a) el nivel de madurez y la eficacia del SGSI b) la penetración de los demás emplazamientos. Además, debe realizarse la evaluación de los emplazamientos de la muestra (Nosamples) 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 prepara los registros y un informe de evaluación preliminar, que explica al contratista durante la llamada Reunión de Cierre. Con la fecha de la reunión de cierre comienza el periodo de 9 meses en el que debe finalizar el proceso de evaluación de TISAX®. Después de la Reunión de Cierre, el contratista elabora el informe de evaluación final (Informe de Initial Assessment) y lo envía al cliente y, a continuación, informa a ENX. En caso de que los resultados lo permitan y no se hayan identificado no conformidades, ENX puede emitir una etiqueta TISAX®.

II. Corrective Action Plan Assessment

Si existen no conformidades tras la realización del Initial Assessment, el cliente debe elaborar un plan de acción (Plan de Acción Correctiva) en un plazo 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 el denominado Corrective Action Plan Assessment, actualiza el informe del Assessment Inicial y genera el informe del Corrective Action Plan Assessment basado en el plan de acción correctiva acordado. El contratista lo enviará al cliente. A continuación, el contratista informa a ENX y, si los resultados lo permiten, ENX puede emitir una etiqueta TISAX® temporal como resultado provisional de la evaluación.

III. Follow-Up Assessment

Si existen no conformidades abiertas tras la finalización del Initial Assessment, se debe coordinar con el contratista un plan de acción para

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. In case this period can not be met, the assessment-process have to be started again from the beginning.

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.

eliminar estas no conformidades y, a continuación, ponerlo en práctica. Posteriormente, a petición del cliente, el contratista lleva a cabo una revisión y evaluación del éxito de la aplicación de las medidas correctoras mediante la realización de un denominado Follow-Up Assessment en función del tipo y el alcance de las no conformidades: en sitio, por teléfono, conferencia web/vídeo/online. A continuación, el contratista prepara el informe final (Follow-Up Assessment Report) (como actualización del Corrective Action Plan Assessment). El contratista lo enviará al cliente. A continuación, 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 han sido efectivamente subsanadas, 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 TISAX® marca el final del proceso de evaluación TISAX®.

El cliente determina a su discreción quién puede ver sus resultados de evaluación en o a través de la plataforma TISAX® de ENX.

5. Información adicional

Un procedimiento TISAX® debe completarse a más tardar nueve meses después de la reunión de cierre. En caso de que no pueda cumplirse este plazo, el proceso de evaluación deberá comenzar de nuevo desde el principio.

Para garantizar la calidad, el contratista lleva a cabo un control de calidad de los informes elaborados por una persona independiente después de cada fase del proceso de evaluación. Se detectan errores o incoherencias y se corrigen o modifican en consecuencia.

6. Obligación de proporcionar información.

A petición de un participante pasivo, el contratista debe proporcionar versiones detalladas del informe con el nivel de detalle solicitado, de conformidad con las normas establecidas por ENX.