

TISAX Participant Handbook

Table of contents

1. Overview
 - 1.1. Purpose
 - 1.2. Scope
 - 1.3. Audience
 - 1.4. Structure
 - 1.5. How to use this document
 - 1.6. Contact us
 - 1.7. The TISAX participant handbook in other languages and formats
 - 1.7.1. About the online format
 - 1.7.2. About the offline format
 - 1.7.3. About the PDF format
2. Introduction
 - 2.1. Why TISAX?
 - 2.2. Who defines what "secure" means?
 - 2.3. The automotive way
 - 2.4. How to prove security efficiently?
3. The TISAX process
 - 3.1. Overview
 - 3.2. Registration
 - 3.3. Assessment
 - 3.4. Exchange
4. Registration (Step 1)
 - 4.1. Overview
 - 4.2. You are a TISAX participant
 - 4.3. Registration preparation
 - 4.3.1. The legal foundation
 - 4.3.2. The TISAX assessment scope
 - 4.3.2.1. Scope description
 - 4.3.2.2. Standard scope
 - 4.3.2.3. Scoping
 - 4.3.2.4. Scope tailoring
 - 4.3.2.5. Scope locations
 - 4.3.2.6. Scope name
 - 4.3.2.7. Contacts
 - 4.3.2.8. Publication and sharing
 - 4.3.3. Assessment objectives
 - 4.3.3.1. List of assessment objectives
 - 4.3.3.2. Assessment objectives and ISA
 - 4.3.3.3. Assessment objectives and TISAX labels
 - 4.3.3.4. Assessment objectives and their dependencies
 - 4.3.3.5. Assessment objective selection
 - 4.3.3.6. Protection needs and assessment levels
 - 4.3.3.7. Assessment objectives and your own suppliers

- 4.3.4. Fee
- 4.4. ENX portal
- 4.5. Online registration process
 - 4.5.1. Time required
 - 4.5.2. Start here
 - 4.5.3. Portal account
 - 4.5.4. Participant registration
 - 4.5.5. Participant contact
 - 4.5.6. General Terms and Conditions
 - 4.5.7. Assessment scope registration
 - 4.5.8. Confirmation email
 - 4.5.8.1. Participant ID
 - 4.5.8.2. Scope ID
 - 4.5.9. Status information
 - 4.5.10. Changes of your registration information
- 5. Assessment (Step 2)
 - 5.1. Overview
 - 5.2. Self-assessment based on the ISA
 - 5.2.1. Download the ISA document
 - 5.2.2. Understand the ISA document
 - 5.2.2.1. Criteria catalogues
 - 5.2.2.2. Chapters
 - 5.2.2.3. Control questions
 - 5.2.2.4. Self-assessment form fields
 - 5.2.2.5. Objective
 - 5.2.2.6. Requirements
 - 5.2.2.7. Maturity levels
 - 5.2.3. Conduct the self-assessment
 - 5.2.4. Interpret the self-assessment result
 - 5.2.4.1. Analysis
 - 5.2.4.2. The target maturity level (on question level)
 - 5.2.4.3. Your result (on question level)
 - 5.2.4.4. The target (on score level)
 - 5.2.4.5. Your result (on score level)
 - 5.2.4.6. Are you ready?
 - 5.2.5. Address the self-assessment result
 - 5.3. Audit provider selection
 - 5.3.1. Contact information
 - 5.3.2. Coverage
 - 5.3.3. Requesting offers
 - 5.3.4. Evaluating offers
 - 5.4. TISAX assessment process
 - 5.4.1. Overview
 - 5.4.2. Kick-off meeting
 - 5.4.3. TISAX assessment types
 - 5.4.4. TISAX assessment elements
 - 5.4.5. About conformity
 - 5.4.6. Your preparation for the TISAX assessment process

- 5.4.7. Initial assessment
 - 5.4.7.1. The first formal opening meeting
 - 5.4.7.2. Assessment procedure
 - 5.4.7.3. Closing meeting
 - 5.4.7.4. TISAX assessment report
- 5.4.8. Corrective action plan preparation
- 5.4.9. Corrective action plan assessment
 - 5.4.9.1. Reasons for a corrective action plan assessment
 - 5.4.9.2. Combination with initial assessment
 - 5.4.9.3. Corrective action plan requirements
 - 5.4.9.4. Temporary TISAX labels
- 5.4.10. Follow-up assessment
 - 5.4.10.1. Timing
 - 5.4.10.2. Prerequisites
 - 5.4.10.3. Expiration of temporary TISAX labels
- 5.4.11. TISAX assessment process diagram
- 5.4.12. Assessment ID
- 5.4.13. TISAX assessment report
- 5.4.14. TISAX labels
 - 5.4.14.1. TISAX label hierarchy
 - 5.4.14.2. Validity period of TISAX labels
 - 5.4.14.3. Renewal of TISAX labels
- 6. Exchange (Step 3)
 - 6.1. Premise
 - 6.2. The exchange platform
 - 6.3. General prerequisites
 - 6.4. Permanence of exchanged results
 - 6.5. Sharing levels
 - 6.6. Publish your assessment result on the exchange platform
 - 6.7. Share your assessment result with a particular participant
 - 6.7.1. Prerequisites
 - 6.7.2. How to create a sharing permission
 - 6.8. Sharing your assessment result outside TISAX
 - 6.8.1. The reasons for the strict governing of the exchange mechanism
 - 6.8.2. A guide to writing about TISAX in public
 - 6.8.3. Sharing with a partner who is not yet a TISAX participant
 - 6.8.4. Sharing with employees of your partner who have no direct access to the ENX portal
- 7. Annexes
 - 7.1. Annex: Example invoice
 - 7.2. Annex: Example confirmation email
 - 7.3. Annex: Example TISAX Scope Excerpt
 - 7.4. Annex: Participant status
 - 7.4.1. Overview: Participant status
 - 7.4.2. Participant status "Incomplete"
 - 7.4.3. Participant status "Awaiting approval"
 - 7.4.4. Participant status "Preliminary"
 - 7.4.5. Participant status "Registered"
 - 7.4.6. Participant status "Expired"

7.5. Annex: Assessment scope status

- 7.5.1. Overview: Assessment scope status
- 7.5.2. Assessment scope status "Incomplete"
- 7.5.3. Assessment scope status "Awaiting your order"
- 7.5.4. Assessment scope status "Awaiting ENX approval"
- 7.5.5. Assessment scope status "Awaiting your payment"
- 7.5.6. Assessment scope status "Registered"
- 7.5.7. Assessment scope status "Active"
- 7.5.8. Assessment scope status "Expired"

7.6. Annex: Assessment status

- 7.6.1. Overview: Assessment status
- 7.6.2. Assessment status "Initial assessment ordered"
- 7.6.3. Assessment status "Initial assessment ongoing"
- 7.6.4. Assessment status "Waiting for corrective action plan assessment"
- 7.6.5. Assessment status "Waiting for follow-up"
- 7.6.6. Assessment status "Finished"

7.7. Annex: The reasoning against "pre-assessments" and "gap analyses"

7.8. Annex: Custom scopes

- 7.8.1. Custom extended scope
- 7.8.2. Full custom scope

7.9. Annex: Participant data life cycle management

- 7.9.1. Lost access to participant data (ENX portal)
- 7.9.2. Administration of contacts
 - 7.9.2.1. How to add a new contact
 - 7.9.2.2. How to delete an existing contact
 - 7.9.2.3. How to update details of an existing contact
- 7.9.3. Administration of locations
 - 7.9.3.1. How to request the change of your company name
 - 7.9.3.2. How to request the change of a location
 - 7.9.3.3. How to request the change of a street name
 - 7.9.3.4. How to add an additional location

7.10. Annex: Scope extension assessment

7.11. Annex: ISA life cycle management

7.12. Annex: Helpful documents

7.13. Annex: Complaint management

- 7.13.1. Causes for complaint
 - 7.13.1.1. Complaints about ENX Association
 - 7.13.1.2. Complaints about audit providers
 - 7.13.1.3. Requirements for complaints
- 7.13.2. Contact for complaints

8. Document history

Get through the TISAX assessment process and share the assessment result with your partner

Published by

ENX Association
an Association according to the French Law of 1901,
registered under No. w923004198 at the Sous-préfecture of Boulogne-Billancourt, France

Addresses

20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, France
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Germany

Author

Florian Gleich

Contact

tisax@enx.com
+49 69 9866927-77

Version

Date: 2023-02-23
Version: 2.5.1
Classification: Public
ENX doc ID: 602

Copyright notice

All rights reserved by ENX Association.
ENX, TISAX, and their respective logos are registered trademarks of ENX Association.
Third party trademarks mentioned are the property of their respective owners.

1. Overview

1.1. Purpose

Welcome to TISAX, the Trusted Information Security Assessment Exchange.

One of your partners requested that you prove that your information security management complies with a defined level according to the requirements of the “Information Security Assessment” (ISA). And now you want to know how to fulfil this request.

The purpose of this handbook is to enable you to fulfil your partner’s request — or to have an edge by anticipating it before a partner asks for it.

This handbook describes the steps you need to take in order to pass the TISAX assessment and for sharing your assessment result with your partner.

Establishing and maintaining an information security management system (ISMS) is already a complex task. Proving to your partner that your information security management is up to the job adds even more complexity. This handbook won’t help you manage your information security. However, it aims to make the work of proving your efforts to your partner as easy for you as possible.

1.2. Scope

This handbook applies to all TISAX processes that you may be part of.

It contains all you need to know to go through the TISAX process.

The handbook offers some advice on how to deal with the information security requirements at the core of the assessment. But it does not aim to generally educate you on what you need to do to pass the information security assessment.

1.3. Audience

The main audience of this handbook are companies that need or want to prove a defined level of information security management according to the requirements of the “Information Security Assessment” (ISA).

As soon as you are actively involved in TISAX processes, you will benefit from the information provided in this handbook.

Companies that are requesting their suppliers to prove defined levels of information security management will benefit, too. This handbook allows them to understand what their suppliers are required to do to fulfil their request.

1.4. Structure

We begin with a brief introduction of TISAX, then we immediately move on with instructions on HOW to do things. You will find all you need to go through the process — in the order you need to know it.

The estimated reading time for the document is 75-90 minutes.

1.5. How to use this document

Sooner or later, you will probably want to understand most of what is described in this document. To be properly prepared, we recommend reading the entire handbook.

We structured the handbook along the three main steps of the TISAX process, so you can go to the section you need and read the rest later.

The handbook uses illustrations to help you improve your understanding. The colours in the illustrations often have additional meaning. We therefore recommend reading the document on a computer screen or as a colour hard copy.

We appreciate your feedback. If you think something is missing in this handbook or is not easy to understand, please don't hesitate to let us know. We and all future readers of this handbook will be thankful for your feedback.

If you have already used a prior version of the TISAX participant handbook, you may find some helpful notes at the end of the document in Section 8, “Document history”.



1.6. Contact us

We're here to guide you through the TISAX process and to answer any questions you may have.

Send us an email at: tisax@enx.com

Or call us at: [+49 69 9866927-77](tel:+4969986692777)






You can reach us during regular business hours in Germany ([UTC+01:00](https://www.worldtimeserver.com/current_time_in_DE.aspx) (https://www.worldtimeserver.com/current_time_in_DE.aspx)).

We all speak  English and  German. One colleague is native speaker of  Italian.

Please take notice of Section 7.13, “Annex: Complaint management”.

1.7. The TISAX participant handbook in other languages and formats

The TISAX participant handbook is available in the following languages and formats:

Language	Version	Format	Link
 English	2.5.1	Online	https://www.enx.com/handbook/tisax-participant-handbook.html (https://www.enx.com/handbook/tisax-participant-handbook.html)
		Offline	https://www.enx.com/handbook/tisax-participant-handbook-offline.html (https://www.enx.com/handbook/tisax-participant-handbook-offline.html)
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf (https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf)
 German	2.5.1	Online	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html (https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html)
		Offline	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html (https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html)
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf (https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf)
 French	2.3 beta	Online	https://www.enx.com/handbook/tph-fr.html (https://www.enx.com/handbook/tph-fr.html)
		Offline	https://www.enx.com/handbook/tph-fr-offline.html (https://www.enx.com/handbook/tph-fr-offline.html)
		PDF	https://www.enx.com/handbook/tph-fr.pdf (https://www.enx.com/handbook/tph-fr.pdf)
 Chinese	2.3 beta	Online	https://www.enx.com/handbook/tph-cn.html (https://www.enx.com/handbook/tph-cn.html)
		Offline	https://www.enx.com/handbook/tph-cn-offline.html (https://www.enx.com/handbook/tph-cn-offline.html)
		PDF	https://www.enx.com/handbook/tph-cn.pdf (https://www.enx.com/handbook/tph-cn.pdf)
 Spanish	2.3 beta	Online	https://www.enx.com/handbook/tph-es.html (https://www.enx.com/handbook/tph-es.html)
		Offline	https://www.enx.com/handbook/tph-es-offline.html (https://www.enx.com/handbook/tph-es-offline.html)
		PDF	https://www.enx.com/handbook/tph-es.pdf (https://www.enx.com/handbook/tph-es.pdf)



Important note:

The English version is the leading version.
All other languages are translations of the English version.
In case of doubt, the English version is authoritative.

1.7.1. About the online format

Each section has a unique ID (format: ID1234).
An ID references a specific section, regardless of the language.
If you want to link to a specific section, you can:

- right-click on the section title and copy the link, or
- click the section title and copy the link from the address bar of your browser.

Most figures are available in a larger size than displayed here by default. Click on the figure to open the larger version.

1.7.2. About the offline format

The offline format retains most features of the online format. Most notably, the figures are embedded in the HTML file. You need only one file to use the offline format.

Compared to the online format, the offline format comes without:

- the larger images
- the original fonts of the online format
Your browser's defaults define the fonts.

1.7.3. About the PDF format

The PDF format is based on the online format. We basically use a browser to save the online format as a PDF.

If you use the PDF format on your computer, you can still click all the references. But if you print the PDF version, you won't have things like page numbers and you will have to look up the references yourself.

2. Introduction

The following sections introduce the TISAX concept.

If you are in a hurry, you can skip them and start right away at Section 4.3, "Registration preparation".

2.1. Why TISAX?

Or rather, why are you here?

In order to answer this question, we will start with some thoughts about doing business in general and protecting information in particular.

Imagine your partner. He has confidential information. He wants to share it with his supplier — you. The cooperation between you and your partner creates value. The information your partner shares with you is an important part of this value creation. Therefore, he wants to protect it appropriately. And he wants to be sure that you are handling his information with the same due care.

But how can he be sure that his information is in good hands? He can't just "believe" you. Your partner needs to see some proof.

Now there are two questions. Who defines what “secure” handling of information means? And next, how do you prove it?

2.2. Who defines what "secure" means?

You and your partner are not the only ones facing these questions for the first time. Almost everyone has to find answers to them and most of the answers will share similarities.

Instead of independently creating a solution for a common problem every time, a standard way of doing it removes the burden of creating everything from scratch. While defining a standard is a huge effort, it is made only once and those who follow it benefit every time.

There are surely different views of what’s the right thing to do for protecting information. But due to the aforementioned benefits, most companies settle on standards. A standard is the condensed form of all proven and time-tested best practices for a given challenge.

In your case, standards like ISO/IEC 27001 (about information security management systems, or ISMS) and their implementation establish a state-of-the-art way to securely handle confidential information. A standard like this saves you from having to reinvent the wheel every time. More importantly, standards provide a common basis when two companies need to exchange confidential data.

2.3. The automotive way

By nature, industry-independent standards are designed as one-size-fits-all solutions rather than tailored to specific needs of automotive companies.

A long time ago, the automotive industry formed associations that aimed — among other goals — to refine and define standards that suit their more specific needs. The “Verband der Automobilindustrie” (VDA) is one of them. In the working group that deals with information security, several members of the automotive industry came to the conclusion that they have similar needs to tailor existing information security management standards.

Their joint efforts led to a questionnaire that covers the automotive industry’s widely accepted information security requirements. It is called the “Information Security Assessment” (ISA).

With the ISA, we now have an answer to the question “Who defines what “secure” means?” Through the VDA, the automotive industry itself offers this answer to its members.

2.4. How to prove security efficiently?

While some companies use the ISA for internal purposes only, others use it to assess the maturity of the information security management of their suppliers. In some cases, a self-assessment is sufficient for the business relationship. However, in certain cases, companies conduct a complete assessment of their supplier’s information security management (including on-site audits).

Along with generally increasing awareness of the need for information security management and the spreading adoption of the ISA as a tool for information security assessments, more suppliers were facing similar requests from different partners.

Those partners still applied different standards and had varying opinions on how to interpret them. But the suppliers essentially had to prove the same things, just in different ways.

And the more suppliers were asked by their partners to prove their level of information security management, the louder their complaints grew in terms of repeat efforts. Showing auditor after auditor the same information security management measures is simply not efficient.

What can be done to make this more efficient? Wouldn't it help if the report of any auditor could be reused for different partners?

OEMs and suppliers in the ENX working group that is responsible for maintaining the ISA listened to their supplier's complaints. Now they offer an answer to their suppliers as well as to all other companies in the automotive industry to the question "How to prove security?"

The answer is TISAX, short for "Trusted Information Security Assessment Exchange".

3. The TISAX process

3.1. Overview

The TISAX process usually^[1] starts with one of your partners requesting that you prove a defined level of information security management according to the requirements of the "Information Security Assessment" (ISA). To comply with that request, you have to complete the 3-step TISAX process. This section gives you an overview of the steps you need to take.

The 3-step TISAX process consists of the following steps:



Figure 1. TISAX process overview

1. Registration

We gather information about your company and what needs to be part of the assessment.

2. Assessment

You go through the assessment(s), which are conducted by one of our TISAX audit providers.

3. Exchange

You share your assessment result with your partner.

Each step consists of sub-steps. These are outlined in the three sections below and described in detail in their respective sections further down.



Please note:

While we would certainly like to tell you how long it will take you to get your TISAX assessment result, we kindly ask for your understanding that it is not possible for us to forecast this in a reliable way. The overall duration of the TISAX process depends on too many factors. The wide variety of company sizes and assessment objectives plus the respective readiness of an information security management system make this impossible.

3.2. Registration

Your first step is the TISAX registration.

The main purpose of the TISAX registration is to gather information about your company. We use an online registration process to help you provide us this information.

It is the prerequisite for all subsequent steps. It is subject to a fee.

During the online registration process:

- We ask you for contact details and billing information.
- You have to accept our terms and conditions.
- You can define the scope of your information security assessment.

For a direct start with this step, please refer to Section 4, “Registration (Step 1)”.

The online registration process is described in detail in Section 4.5, “Online registration process”. But if you want to start right away, please go to enx.com/en-US/TISAX/.

3.3. Assessment

Your second step is going through the information security assessment.

There are four sub-steps:

a. Assessment preparation

You have to prepare the assessment. The extent of this depends on the current maturity level of your information security management system. Your preparation has to be based on the ISA catalogue.

b. Audit provider selection

You have to choose one of our TISAX audit providers.

c. Information security assessment(s)

Your audit provider will conduct the assessment based on an assessment scope that matches your partner’s requirements. The assessment process will consist of the initial audit at a minimum.

If your company does not pass the assessment right away, the assessment process may require additional steps.

d. Assessment result

Once your company passes the assessment, your audit provider will provide you with the official TISAX assessment report. Your assessment result will also receive TISAX labels^[2].

For more information about this step, please refer to Section 5, “Assessment (Step 2)”.

3.4. Exchange

Your third and last step is to share your assessment result with your partner. The content of the TISAX assessment report is structured in levels. You can decide up to which level your partner will have access.

Your assessment result is valid for three years. Assuming you are still a supplier of your partner then, you will have to go through the three-step process again^[3].

For more information about this step, please refer to Section 6, “Exchange (Step 3)”.

Now that you have a fundamental idea about what the TISAX process is, you will find instructions on how to complete each step in the following sections.

4. Registration (Step 1)

The estimated reading time for the registration section is 30-40 minutes.

4.1. Overview

The TISAX registration is your first step. It is the prerequisite for all subsequent steps.

The following sections will guide you through the registration:

1. We start with explaining an essential new term.
2. Then we advise you on what you should do to be prepared for the online registration process.
3. Next, we guide you through the online registration process.

4.2. You are a TISAX participant

Let us first introduce a new term that is necessary to understand. So far, you have been the “supplier”. You are here to fulfil a requirement of your “customer”. TISAX itself however does not really differentiate between these two roles. For TISAX, everyone who registered is a “participant”. You — as well as your partner — “participate” in the exchange of information security assessment results.



Figure 2. Register to become a TISAX participant

To differentiate the two roles from the beginning, we refer to you, the supplier, as “active participant”. We refer to your partner as “passive participant”. As an “active participant” you get TISAX-assessed and you share your assessment result with other participants. The “passive participant” is the one who requested that you get TISAX-assessed. The “passive participant” receives your assessment result.

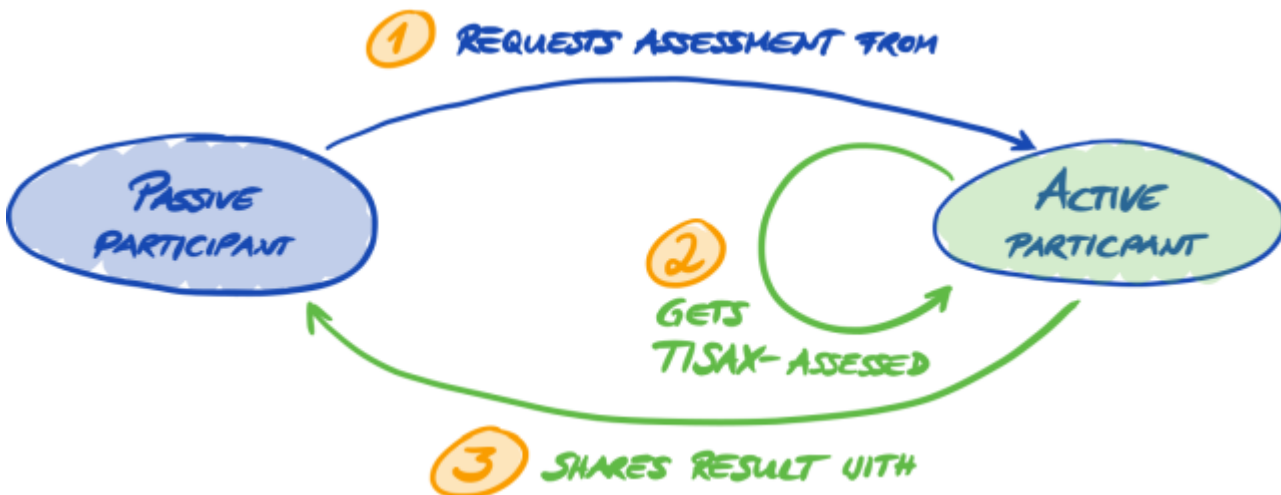


Figure 3. Passive participant and active participant

Any company can act in both roles. You might share an assessment result with your partner, while at the same time requesting your own suppliers to get TISAX-assessed.



Figure 4. TISAX participants can be active and passive at the same time

Requesting your own suppliers to get TISAX-assessed may even be especially advisable if your own suppliers are handling your partner's information with protection needs as well.

4.3. Registration preparation

In this section, we give you recommendations on how to *prepare* for the registration. We describe the registration process itself in detail in Section 4.5, "Online registration process".

Before you start going through our online registration process, we strongly recommend:

- gathering information in advance
- and taking some decisions.


4.3.1. The legal foundation

Typically, you need to sign two contracts. The first contract you enter is between you and ENX Association: The "TISAX Participation General Terms and Conditions" (TISAX Participant GTCs). The second contract is between you and one of our TISAX audit providers. For the registration, we will look at the first contract only.


The TISAX Participant GTCs govern our mutual relationship and your relationship with other TISAX participants. They define the rights and duties for all of us. Besides the usual clauses you will find in most contracts, they define the handling of the information exchanged and obtained during the TISAX process in detail. A key objective of these rules is to keep TISAX assessment results confidential. As all TISAX participants are subject to the same rules, you can expect appropriate protection of your TISAX assessment result by your partner (in his role as passive participant).


Quite early in the online registration process, we will ask you to accept the TISAX Participant GTCs. As this is a real contract, we recommend reading the TISAX Participant GTCs before starting the online registration process. One reason is that depending on your role in your company, you may need to obtain a clearance from an in-house or external lawyer.

You can download the “TISAX Participation General Terms and Conditions”^[4] on our website at:

 enx.com/en-US/TISAX/downloads/

Direct PDF download:

 enx.com/tisaxgtcen.pdf

 enx.com/tisaxgtcde.pdf

During the online registration process, we will ask you to check two mandatory checkboxes:

- We accept the TISAX Participation General Terms and Conditions
- We confirm knowledge of Applicant’s release of Audit Providers’ professional duties of secrecy acc. to Sec. IX.5. and X.3 of the TISAX Participation General Terms and Conditions;

We have the second checkbox because some of our TISAX audit providers are certified public accountants. They have special requirements regarding professional secrecy. Usually, the special requirements regarding professional secrecy prohibit the certified public accountants among our audit providers from sharing information with us. Particularly, this would cancel the control options we need for our governance role. Therefore, we need this release. You may want to pay special attention to those clauses before checking the box.

If you usually require a non-disclosure agreement (NDA) between you and anyone who handles confidential information, please examine the respective sections of our GTCs. They should address all your concerns. Moreover, you usually don’t have to provide us any confidential information at all.

Concluding the legal section, we ask for your understanding that the system depends on everyone accepting the same rules. We therefore can’t accept any additional general terms and conditions^[5].

4.3.2. The TISAX assessment scope

In the second step of the TISAX process, one of our TISAX audit providers will conduct the information security assessment. He needs to know where to start and where to stop. That’s why you need to define an “assessment scope”.

The “assessment scope” describes the scope of the information security assessment. In simple terms, every part of your company that handles your partner’s confidential information is part of the assessment scope. You can consider it a major element of the audit provider’s task description. It dictates what the audit provider needs to assess.

The assessment scope is important for two reasons:

- a. An assessment result will only fulfil your partner’s requirement if the respective assessment scope covers all parts of your company that handle partner information.
- b. A precisely defined assessment scope is an essential prerequisite for meaningful cost calculations by our TISAX audit providers.



Important note:

ISO/IEC 27001 vs. TISAX

First, we have to differentiate two types of scopes:

- 1) the scope of your information security management system (ISMS) and
- 2) the scope of the assessment.

These two are not necessarily identical.

For the ISO/IEC 27001 certification, you define the scope of your ISMS (in the “scope statement”). You are completely free to define the scope of your ISMS. However, the scope of the assessment (also known as “audit scope”) must be identical with the scope of your ISMS.

For TISAX, you also have to define your ISMS. But the scope of the assessment can be different.

For the ISO/IEC 27001 certification, you can freely shape the scope of the assessment through the way you define the scope of your ISMS.

In contrast, for TISAX, the scope of the assessment is predefined. The scope of the assessment can be smaller than the scope of your ISMS. But it must be within the scope of your ISMS.

4.3.2.1. Scope description

The scope description defines the assessment scope. For the scope description, you have to choose one of two scope types:

1. Standard scope
2. Custom scope
 - a. Custom extended scope
 - b. Full custom scope

We discuss the standard scope in the following section. The standard scope is the right choice for well over 99% of all participants. Therefore, we only discuss the custom scopes in Section 7.8, “Annex: Custom scopes”.

4.3.2.2. Standard scope

The standard scope description is the basis for a TISAX assessment. Other TISAX participants only accept assessment results based on the standard scope description.

The standard scope description is predefined and you can’t change it.

A major benefit of having a standard scope is that you don’t have to come up with your own definition.

This is the standard scope description (version 2.0):

The TISAX scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations. The assessment is conducted at least in the highest assessment level listed in any of the listed assessment objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

We strongly recommend choosing the standard scope. All TISAX participants accept information security assessment results based on the standard scope.

4.3.2.3. Scoping

Your next task after defining the scope type is to decide which locations belong to the assessment scope.

If your company is small (one location), this is an easy task. You simply add your location to the assessment scope.

If your company is large, you can consider registering more than one assessment scope.

Having a single scope that contains all your locations has advantages:

- You have one assessment report, one assessment result, one expiration date.
- You can benefit from reduced costs for the assessment because a TISAX audit provider only has to assess your central processes, procedures and resources once.

But a single scope may have disadvantages such as:

- All locations must have the same assessment objectives.
- The assessment result is only available once the TISAX audit provider has assessed all locations. This fact may be relevant if you urgently need an assessment result.
- The assessment result depends on all locations passing the assessment. If just one location fails, you won't have a positive assessment result. A workaround for this is to: a) remove the location from the scope, b) solve the issues, c) add the location afterwards with a scope extension assessment.

4.3.2.4. Scope tailoring

The question whether to have just one scope or several scopes is one that only you can answer. But answering the questions in the following diagram may help you decide.

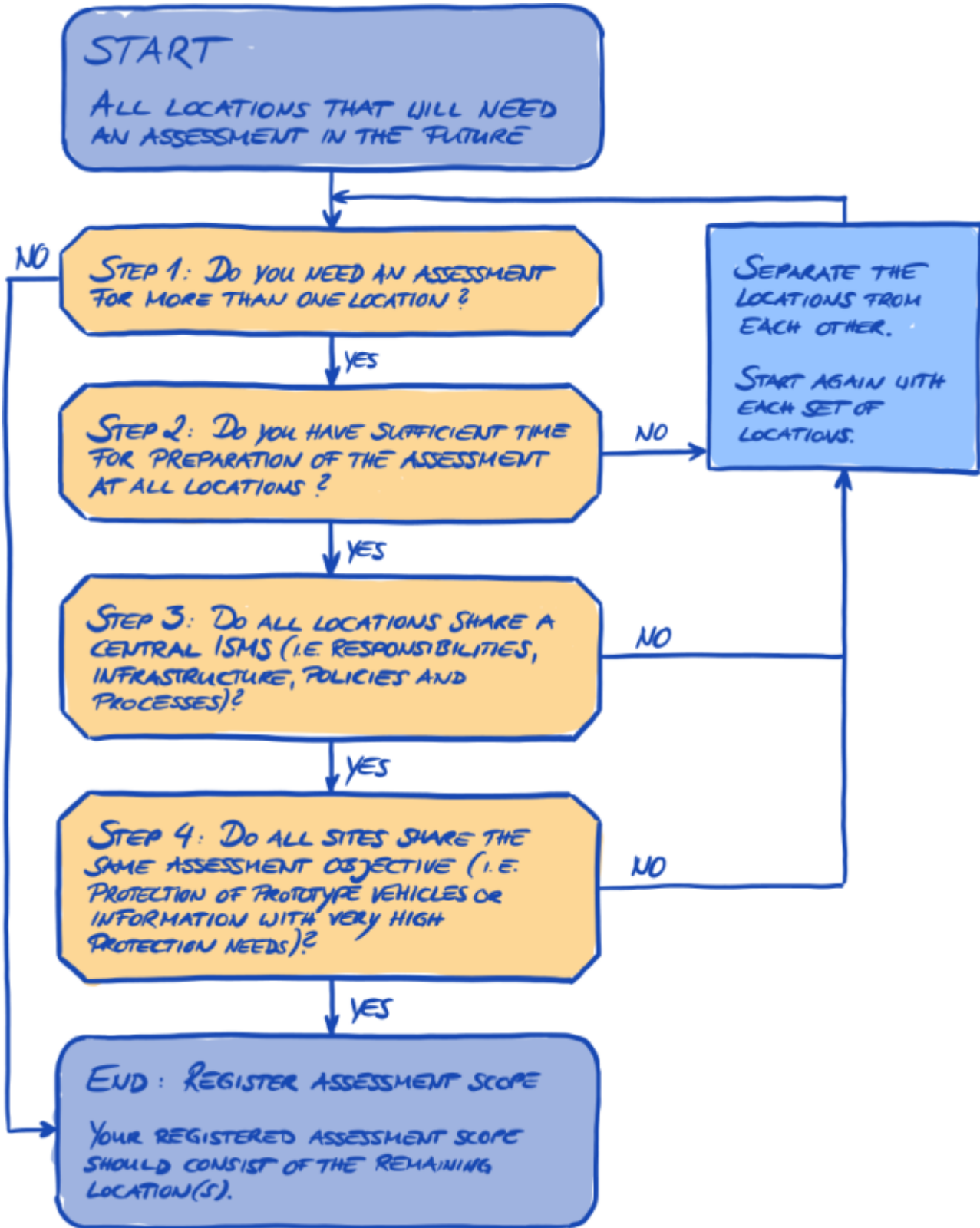


Figure 5. Scope tailoring decision tree



Please note:

Don't let this decision intimidate you. You can change any scope as long as the audit provider didn't conclude the assessment.

For example, during your assessment preparation you may find that the scope does not fit — and change it accordingly. Or your audit provider may recommend changing the scope during the earlier stages of the assessment.

Additional notes:

- Technically, you can't change the assessment scope that you defined during the online registration process in the ENX portal. But the audit provider can update your assessment scope when he uploads your assessment result to the ENX portal.
- Adding to the scope increases the fee and you won't get a refund if you remove locations from the scope. Since the audit providers use the original scope as a basis for their cost calculation, you should also expect changes.

4.3.2.5. Scope locations

Now that you have decided which locations are part of your assessment scope, you can continue gathering some location-specific information.

For each location we ask for information like company name and address. We also ask for some additional information that allows our TISAX audit providers to get a better idea of your company structure. Your answers will be the basis of their effort estimations.

Please prepare yourself to provide the following details for each of your locations (the red asterisk * indicates mandatory information in the online process):

Field	Options
Location Name *	n/a
<u>D&B D-U-N-S NUMBER</u> (https://en.wikipedia.org/wiki/Data_Universal_Numbering_System)	n/a
Location Type *	Building(s) owned and used exclusively by company Building(s) rented by company Floor/office rented by company in a shared building Office shared with other companies Own Datacenter Shared Datacenter
Passive Site Protection *	Yes No

Field	Options
Industry <i>(Several selections possible)</i>	<p>Information Technology</p> <ul style="list-style-type: none"> <input type="checkbox"/> IT Services <input type="checkbox"/> Telecommunication Services <input type="checkbox"/> Software Development <p>Management</p> <ul style="list-style-type: none"> <input type="checkbox"/> Consulting <p>Media</p> <ul style="list-style-type: none"> <input type="checkbox"/> Marketing <input type="checkbox"/> Agency <input type="checkbox"/> Printing Services <input type="checkbox"/> Photography <input type="checkbox"/> Translation Services <p>Research And Development</p> <ul style="list-style-type: none"> <input type="checkbox"/> Vehicle Testing <input type="checkbox"/> Vehicle Simulation <input type="checkbox"/> Prototype Construction <input type="checkbox"/> Miniature Car Models <input type="checkbox"/> Development Services <input type="checkbox"/> CAx Development Services <p>Production</p> <ul style="list-style-type: none"> <input type="checkbox"/> Production Services <input type="checkbox"/> Contract Manufacturing <input type="checkbox"/> Shop Floor <input type="checkbox"/> Logistics <p>Sales And Aftersales</p> <ul style="list-style-type: none"> <input type="checkbox"/> Import, NSC <input type="checkbox"/> Dealership <input type="checkbox"/> Financial Services <input type="checkbox"/> Insurance <input type="checkbox"/> Claims Settlement

Field	Options
	Other Industry <i>(please enter)</i>
Employees at Location: Overall *	0 1-10 11-100 101-1.000 1.001-5.000 More than 5.000
Employees at Location: IT *	0 1-10 11-25 26-50 More than 50
Employees at Location: IT Security *	0 Part Time 1-5 6-25 More than 25
Employees at Location: Location Security *	0 Part Time 1-3 4-10 More than 10
Certifications for this Location	ISO 27001 Other <i>(please enter)</i> ISAE 3402 SOC2

Table 1. Location-specific details



Please note:

Regarding the “Industry”: Select to the best of your knowledge. There is no right or wrong when selecting from the options above. If you can’t find an option that matches your type of business, just enter the appropriate option under “Other”.

For each location you have to specify a “location name”. The purpose of the location name is to make it easier to refer to the location when you assign them to an assessment scope.

We recommend assigning location names based on the following pattern:

Pattern: [Geographical reference]

Example: for the fictitious company “ACME”

- **Frankfurt**
(for a location in the German **city** Frankfurt)

4.3.2.6. Scope name

For each scope, you have to specify a “scope name”. The main purpose of the scope name is to make it easy for you to identify a scope in the overview list of scopes in the ENX portal. You should assign a name that is helpful to the reader and your colleagues. For external communication, you should use the Scope ID.

You can specify any name you want. But you shouldn’t assign the same scope name for more than one scope.

When you later want to renew your TISAX assessment, you need to create a new scope (possibly identical to the current scope). We therefore recommend adding the year of the assessment to the scope name.

We recommend assigning scope names based on the following pattern:

Pattern: **[Geographical or *functional* reference]** **[Year of the assessment]**

Examples: for the fictional company “ACME”

- **2020**
(without geographical reference if your company has just one location)
- **Frankfurt 2020**
(for a scope with several locations in the German **city** of Frankfurt)
- **Lower Saxony 2020**
(for a scope with all locations in the German **state** of Lower Saxony)
- **Germany 2020**
(for a scope with all locations in the **country** of Germany)
- **EMEA 2020**
(for a scope with all locations in the EMEA **region** (“Europe, Middle East, Asia”))
- **Prototype development 2020**
(*functional* reference for a scope with all locations involved in developing prototypes)

4.3.2.7. Contacts

In order to communicate with you, we collect information about contacts at your company.

We ask for at least one contact for your company as TISAX participant in general and one for each assessment scope. You have the option to provide additional contacts.

During your registration preparations, you should decide who at your company will be a contact.

We ask for the following contact details:

	Contact detail	Mandatory?	Example
1.	Salutation	Yes	Mrs., Mr.
2.	Academic degree		Dr., Ph.D., other

	Contact detail	Mandatory?	Example
3.	First name	Yes	John
4.	Last name	Yes	Doe
5.	Job title	Yes	Head of IT
6.	Department	Yes	Information Technology
7.	Primary phone number	Yes	+49 69 986692777
8.	Secondary phone number		
9.	Email address	Yes	john.doe@acme.com
10.	Preferred language	Yes	English (default)
11.	Other languages		German, French
12.	Personal address identifier		HPC 1234
13.	Street address	Yes	Bockenheimer Landstraße 97-99
14.	Postal code	Yes	60325
15.	City	Yes	Frankfurt
16.	State/Province		
17.	Country	Yes	Germany

Table 2. Contact details



Important note:

We recommend assigning at least one alternate for each contact. If a contact is temporarily unavailable or leaves the company, someone else can manage your company's participant data. If you need to assign a new contact (without any other remaining valid contacts), you have to go through a complex process. Our process ensures that only persons who can prove that they are entitled to legally represent the company can approve assigning a new main contact.

4.3.2.8. Publication and sharing

The main purpose of TISAX is to publish your assessment result to other TISAX participants and to share your assessment result with your partner(s).

You can decide about the publication and sharing of your assessment result either during the registration process or at any time later.

If you are going through the TISAX process as a pre-emptive step, you can already decide to publish your assessment result to the community of TISAX participants. Otherwise, there is nothing to prepare for at this stage.

If your partner requested that you to go through the TISAX process, you need to share your assessment result sooner or later. You can already share status information with your partner during the registration. Once your assessment result is available, your partner will then automatically have the permission to access it^[6].

There are two things you need to share status information:

1. Your partner's TISAX Participant ID

The TISAX Participant ID identifies your partner as a TISAX participant.

Usually, your partner should provide you his TISAX Participant ID.

For your convenience, our registration form provides a drop-down list of Participant IDs for some companies that frequently receive shared assessment results.^[7]

2. The required sharing level

The sharing level defines the depth to which your partner can access your assessment result.

Either your partner requests a specific sharing level or you decide up to which level you want to grant your partner access to your assessment result.

For more information on sharing levels, please refer to Section 6.5, "Sharing levels".

So you may want to make sure you have this information.



Please note:

- You can always decide to publish your assessment result later.
- You can always create a sharing permission for your partner later.



Important note:

If you don't publish your assessment result or don't share it, no one can see your assessment result.



Important note:

You can't revoke publication or sharing.

For details, please refer to Section 6.4, "Permanence of exchanged results".



Please note:

It may sound odd, but you can in fact share your "assessment result" even if haven't started the assessment process yet. At this early stage, you are just sharing the "assessment status". The participant with whom you share your "assessment result" will see where you are in the assessment process.

Some TISAX participants have to issue a special release if you have to show TISAX labels, but haven't finished the assessment process yet. In such a case, your partner may need to see your "assessment status" in his account for the ENX portal.

For more information on the assessment status, please refer to Section 7.6, "Annex: Assessment status".

For more information on publishing and sharing your assessment result, please refer to Section 6, "Exchange (Step 3)".

4.3.3. Assessment objectives

You have to define your assessment objective(s) during the registration process. The assessment objective determines the applicable requirements that your information security management system (ISMS) has to fulfil. The assessment objective is entirely based on the type of data you handle on behalf of your partner.

In the following sections, we describe the assessment objectives and provide advice on how to select the right assessment objective(s).

The use of assessment objectives makes the TISAX-related communication with your partner and our TISAX audit providers easier because they refer to a defined input to the TISAX assessment process.



Please note:

Some partners may request you to get TISAX-assessed with a certain “assessment level” (AL) instead of specifying an assessment objective. For more information on assessment levels, please refer to Section 4.3.3.6, “Protection needs and assessment levels” (sub-section “Additional information”).

4.3.3.1. List of assessment objectives

There are currently eight TISAX assessment objectives. You have to select at least one assessment objective. You may select more than one.

Consider your assessment objective the benchmark for your information security management system. The assessment objective is a key input for the TISAX process. All TISAX audit providers base their assessment strategy mainly on the assessment objective.

The current TISAX assessment objectives are:

No.	Assessment objective	Abbreviation
1.	Handling of information with high protection needs	Info high
2.	Handling of information with <u>very</u> high protection needs	Info <u>very</u> high
3.	Protection of prototype parts and components	Proto parts
4.	Protection of prototype vehicles	Proto vehicles
5.	Handling of test vehicles	Test vehicles
6.	Protection of prototypes during events and film or photo shoots	Proto events
7.	Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	Data
8.	Data protection with <u>special</u> categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	<u>Special</u> data

Table 3. The current TISAX assessment objectives

Example: If you are conducting test drives on public roads, then the assessment objective No. 5 “Handling of test vehicles” is one of your assessment objectives.

For some of the following illustrations, we will use a table representation of the eight TISAX assessment objectives. Furthermore, we will shorten the long forms for an easier visual representation.

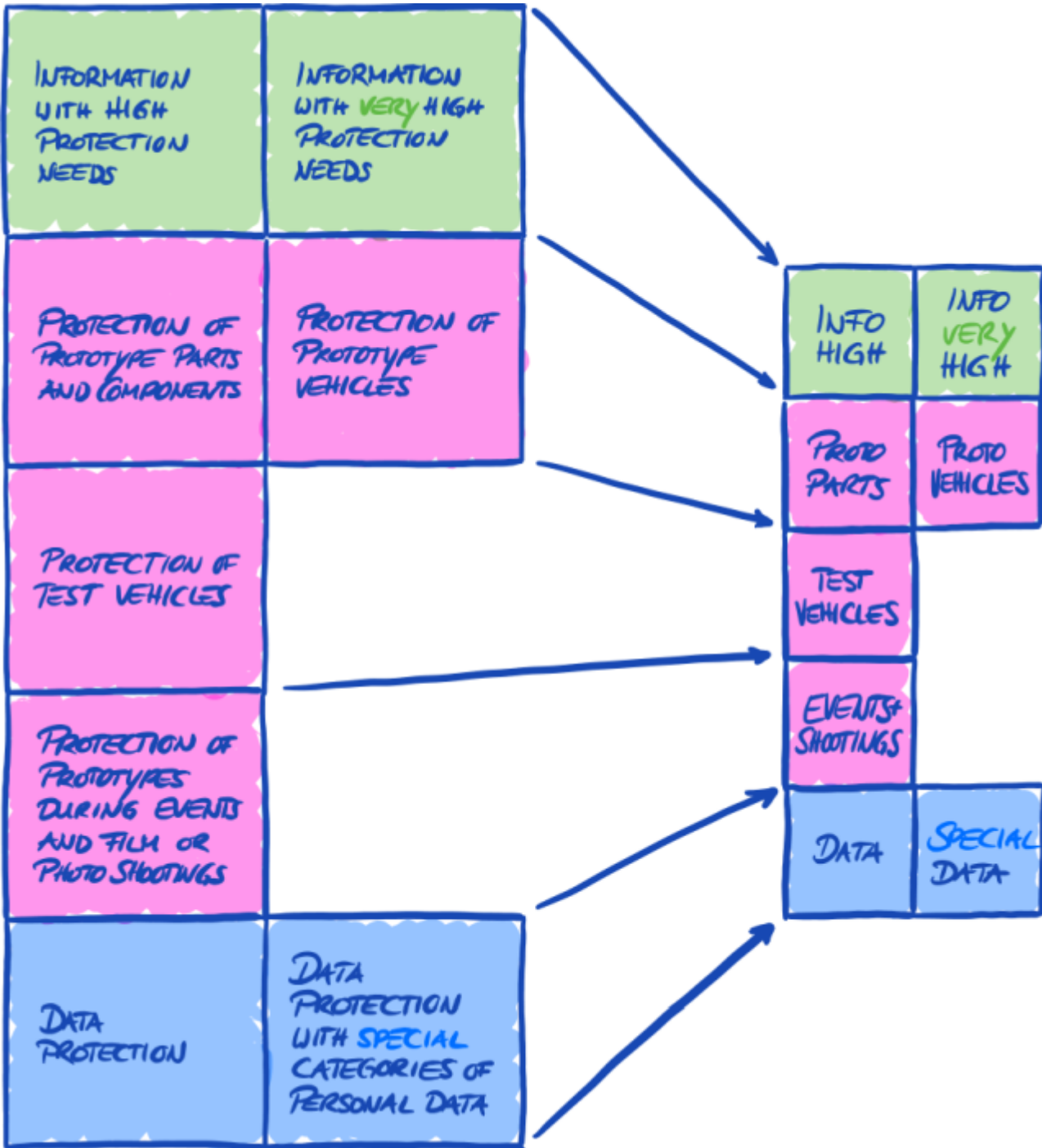


Figure 6. TISAX assessment objectives (table representation, long and short forms)



Important note:

Within TISAX, the “assessment objective” is generally the process input. However, some partners may request you to get TISAX-assessed with a certain “assessment level” (AL).

For more information on the relationship between protection needs and assessment levels, please refer to Section 4.3.3.6, “Protection needs and assessment levels”.

4.3.3.2. Assessment objectives and ISA

Each assessment objective maps to a criteria catalogue of the ISA.

Example: Both “Information” assessment objectives with high or very high protection needs map to the criteria catalogue “Information Security” of the ISA. The Excel sheet is the same for both assessment objectives. Depending on the protection needs, either the column “Additional requirements for high protection needs” or the column “Additional requirements for very high protection needs” applies.

For further background information on the TISAX assessment objectives regarding their relationship to the ISA criteria catalogues and the assessment levels, please refer to Section 5.2.2, “Understand the ISA document”.

4.3.3.3. Assessment objectives and TISAX labels

Your partner may speak of “TISAX labels”. “Assessment objectives” and “TISAX labels” are almost the same. The difference is that you start into the assessment process with the “assessment objectives” and if you pass the assessment you receive the corresponding “TISAX labels”.

Example: Your partner requires you to get the TISAX label “Handling of information with high protection needs”. Then you select “Handling of information with high protection needs” as your assessment objective.

The figure below shows you the input and output of the TISAX process:

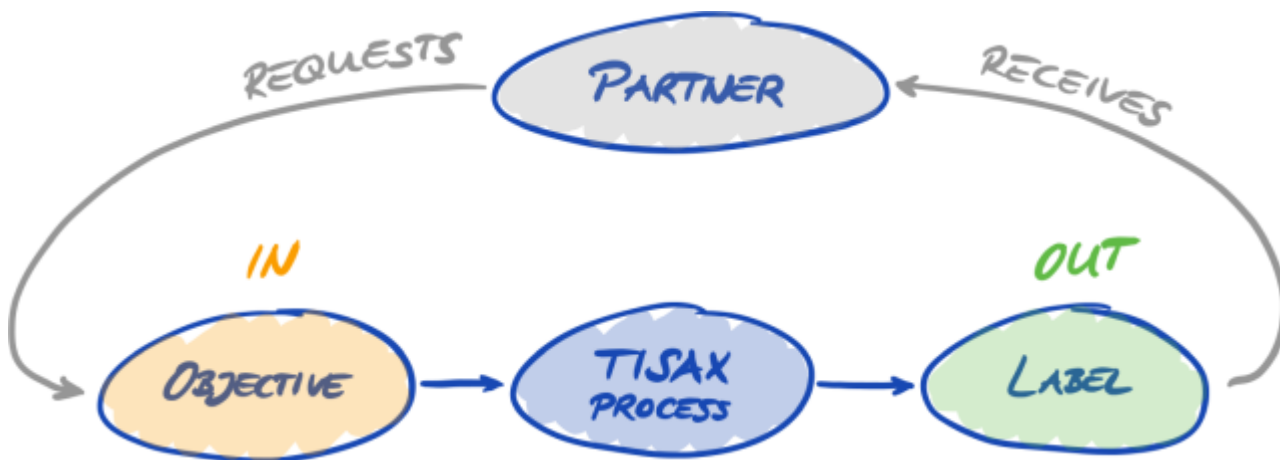


Figure 7. Assessment objectives and TISAX labels

For more information on TISAX labels, please refer to Section 5.4.14, “TISAX labels”.

4.3.3.4. Assessment objectives and their dependencies

The assessment objective “Handling of information with high protection needs” is the minimum for a TISAX assessment. Additional assessment objectives are optional. However, depending on the information you handle, you may have to add further assessment objectives. You will find more information on which assessment objectives you may need further down.

Some assessment objectives have dependencies with other assessment objectives. Either the assessment objective “Handling of information with high protection needs” or “Handling of information with very high protection needs” is the basis for all other assessment objectives.

Example: If you need to achieve the assessment objective “Protection of prototype parts and components”, then you have to also automatically achieve the assessment objective “Handling of information with high protection needs”. You will find more information about the dependencies further down.

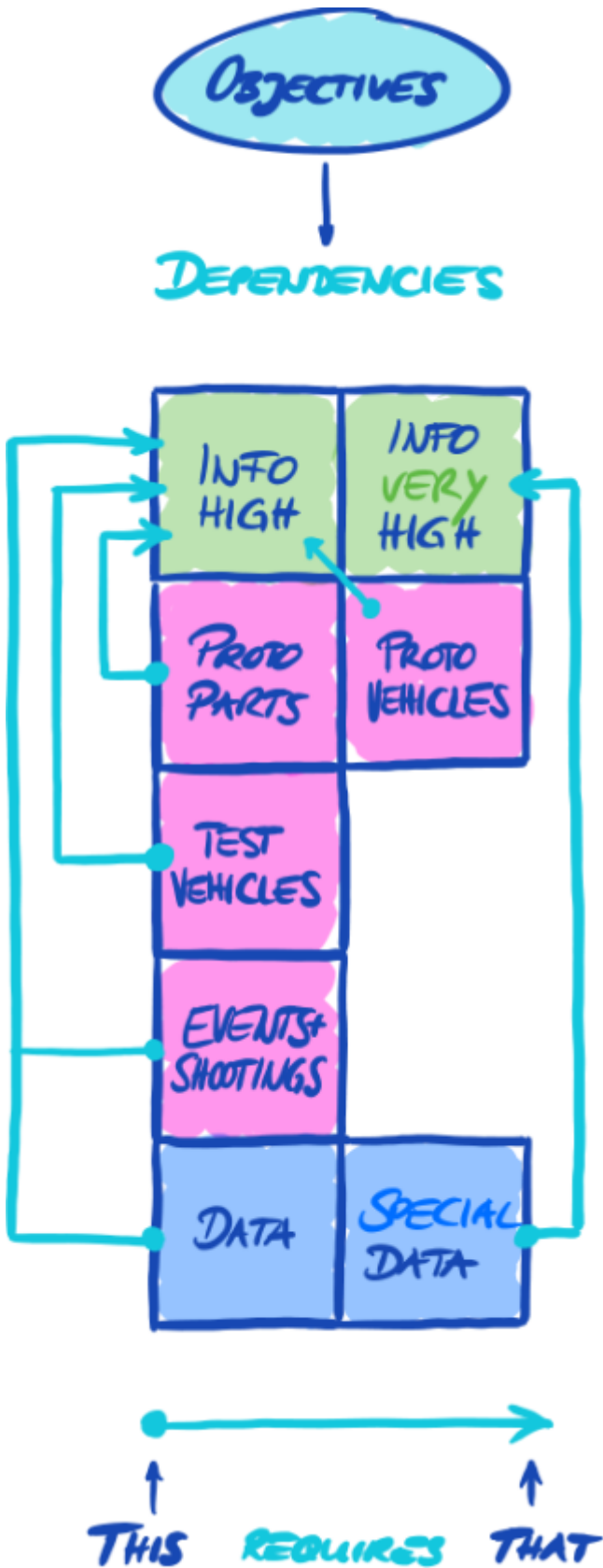


Figure 8. The assessment objectives and their dependencies

4.3.3.5. Assessment objective selection

Ideally, your partner tells you precisely which assessment objectives you have to achieve.

You have to select the assessment objective based on your own judgement if:

- you want to get TISAX-assessed before a partner asks for it, or
- your partner does not tell you which assessment objective to achieve.



Important note:

At this point, we strongly recommend considering your other partners. Are there existing partners that have the same or higher requirements? Do you expect future partners to have higher requirements?

You may want to consider selecting assessment objectives with a higher protection needs. Doing so prevents issues when other partners have higher requirements.

If you have to select the assessment objective based on your own judgement, you may find it helpful to consider the following aspects:

No.	Assessment objective	Information
1.	Handling of information with high protection needs (Info high)	You may derive the protection needs (high, <u>very</u> high) from the document classification of your partner.
2.	Handling of information with <u>very</u> high protection needs (Info <u>very</u> high)	
3.	Protection of prototype parts and components (Proto parts)	For all companies that manufacture, store or use customer-provided components or parts classified as requiring protection at their own locations. Requirements for physical security and for security considering the surrounding area, organisational requirements and specific requirements for handling prototypes are part of the assessment.
4.	Protection of prototype vehicles (Proto vehicles)	For all companies that manufacture, store or use customer-provided vehicles classified as requiring protection at their own locations. Requirements for physical security and for security considering the surrounding area (including the existence of protected garages and workshop areas), organisational requirements and specific requirements for handling prototypes are part of the assessment. After a successful assessment, you automatically receive the TISAX label "Protection of prototype parts and components".

No.	Assessment objective	Information
5.	Handling of test vehicles (Test vehicles)	<p>For all companies that conduct tests and test drives (e.g. test drives on public roads or test tracks) with customer-provided vehicles classified as requiring protection.</p> <p>Organisational requirements, specific requirements for handling prototypes incl. camouflage and handling of vehicles during test drives in public and on test tracks are part of the assessment.</p> <p>Requirements for physical security and for security considering the surrounding area are not necessarily part of the assessment. If your locations are equipped accordingly, we recommend also selecting the assessment objective “Protection of prototype vehicles”.</p>
6.	Protection of prototypes during events and film or photo shoots (Proto events)	<p>For all companies that conduct presentations or events (e.g. market research, events, marketing events) and film and photo shootings with customer-provided vehicles, components or parts classified as requiring protection.</p> <p>Organisational requirements and specific requirements for handling prototypes incl. requirements for presentations, events and film and photo shootings in protected rooms and in public are part of the assessment.</p> <p>Requirements for physical security and for security considering the surrounding area are not necessarily part of the assessment. If your locations are equipped accordingly, we recommend also selecting the assessment objective “Protection of prototype vehicles”.</p>
7.	Data protection (Data)	If you handle personal data as a processor according to Article 28 of the GDPR, you probably have to select “Data protection”.
8.	Data protection with <u>special</u> categories of personal data (<u>Special</u> data)	If you handle special categories of personal data (like health or religion) as a processor according to Article 28 of the GDPR, then you probably have to select “Data protection with <u>special</u> categories of personal data”.

Table 4. Advice for selecting an assessment objective

Further explanations:

- If you have precise requirements from your partner, you usually don't need to discuss your assessment objectives with your partner. However, if you don't have precise requirements from your partner, we strongly recommend consulting your partner before initiating the assessment process.
- The ISA describes the implementation difference between “high” and “very high” protection needs (if there is any) for each requirement.
For more information on this, please refer to Figure 13, “Screenshot: Main elements of the questions in the ISA criteria catalogues”.

4.3.3.6. Protection needs and assessment levels

Your partner has various types of information, of which some may deserve a higher level of protection than others. The ISA accommodates this by differentiating three “protection needs”: normal, high and very high. Your partner classifies his information and usually assigns protection needs.

The TISAX assessment objectives pair an ISA criteria catalogue with either “high” or “very high” protection needs.

No.	ISA criteria catalogue	Protection needs	TISAX assessment objective
1.	Information security	high	Handling of information with high protection needs
2.	Information security	<u>very</u> high	Handling of information with <u>very</u> high protection needs
3.	Prototype protection	high	Protection of prototype parts and components
4.	Prototype protection	high	Protection of prototype vehicles
5.	Prototype protection	high	Handling of test vehicles
6.	Prototype protection	high	Protection of prototypes during events and film or photo shoots
7.	Data protection	high	Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)
8.	Data protection	<u>very</u> high	Data protection with <u>special</u> categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)

Table 5. Mapping of ISA criteria catalogues and protection needs to TISAX assessment objectives

The higher the protection needs, the more your partner is interested in making sure that it is safe to let you handle their information. Therefore, TISAX differentiates three “assessment levels” (AL). The assessment level defines which assessment method the audit provider has to apply. A higher assessment level increases the effort that goes into the assessment. This results in greater care and accuracy in the assessment.

The table below shows you the assessment levels that apply to the TISAX assessment objectives:

No.	TISAX assessment objective	Assessment level (AL)
1.	Handling of information with high protection needs	AL 2
2.	Handling of information with <u>very</u> high protection needs	AL <u>3</u>
3.	Protection of prototype parts and components	AL 3
4.	Protection of prototype vehicles	AL 3
5.	Handling of test vehicles	AL 3
6.	Protection of prototypes during events and film or photo shoots	AL 3

No.	TISAX assessment objective	Assessment level (AL)
7.	Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	AL 2
8.	Data protection with <u>special</u> categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	AL <u>3</u>

Table 6. Mapping of the TISAX assessment objectives to assessment levels

Assessment level 1 (AL 1):

Assessments in assessment level 1 are mainly for internal purposes in the true sense of a self-assessment.

For an assessment in assessment level 1, an auditor checks for the existence of a completed self-assessment. He does not assess the content of the self-assessment. He does not require further evidence.

Results of assessments in 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.

Assessment level 2 (AL 2):

For an assessment in assessment level 2, the audit provider does a plausibility check on your self-assessment (for all locations within the assessment scope). He supports this by checking evidence^[8] and conducting an interview with the person in charge information security.

The audit provider does the interview generally via web conference. At your request, he can conduct the interview in person.

If you have evidence you don't want to send to the audit provider, you can request an on-site inspection. In this way, the audit provider can still check your “for your eyes only” evidence.



Please note:

There is an alternate method to conduct an assessment in assessment level 2. Instead of the plausibility check, the audit provider conducts a full remote assessment. This method is sometimes referred to as “**assessment level 2.5**”.

Compared to an assessment in assessment level 2, the auditor *verifies* whether your ISMS fulfils the applicable requirements. Yet in contrast to an assessment in assessment level 3, the auditor does not conduct the on-site activities outlined in the section about assessment level 3 below.

Formally, such an assessment will be evaluated as an assessment in AL 2.

The advantage of AL 2.5 is that the approach is methodically compatible with AL 3. It is therefore possible to upgrade to a fully-fledged assessment in AL 3 with a manageable effort at a later point in time. For the upgrade, the auditor only has to conduct the on-site activities outlined in the section about AL 3 below.

We recommend assessments in assessment level 2.5 in these cases:

1. You currently only need TISAX labels that imply an assessment in AL 2, but you can't exclude the possibility that other partners may require TISAX labels that imply an assessment in AL 3. An assessment in AL 2.5 keeps the way open to later upgrade to AL 3.
2. You have difficulties to compile a sufficiently plausible self-assessment. For the plausibility check, the self-assessment has to be conclusive, well comprehensible and substantiated. Compiling such a self-assessment can cause considerable internal effort, even for companies that are fundamentally well positioned.

For more information on upgrading the assessment level, please refer to Section 7.10, “Annex: Scope extension assessment”.

This alternative is optional and not required to fulfil the AL 2 requirements. The difference between AL 2 and AL 2,5 won't be visible for partners with whom you share your assessment result.

Assessment level 3 (AL 3):

For an assessment in assessment level 3, the audit provider does a comprehensive verification of your company's compliance with the applicable requirements. The auditor uses your self-assessment and submitted documentation to prepare the assessment. But in contrast to assessment level 2, the auditor will verify everything. He will:

- examine documents and evidence
- conduct planned interviews with process owners.
- observe local conditions
- observe the execution of processes
- conduct *unplanned* interviews with process participants



Please note:

The following text refers to several concepts that will be explained only later in this document.

With AL 3, the audit provider must come to your location(s). If, for some reason, this is temporarily not possible at all or would require unreasonable efforts, your audit provider can use the **video-supported remote assessment method** to conduct the on-site activities of the assessment.

Your audit provider has to record this in the TISAX assessment report as a minor non-conformity. As soon as your audit provider can come to your location(s), he must conduct a follow-up assessment that includes all previously impossible on-site activities. Furthermore, you have to schedule the follow-up assessment even if you haven't yet completed the other corrective actions.

Compared to waiting for your audit provider's availability for on-site activities, this approach allows you to already share temporary TISAX labels with your partner.

Assessment levels and assessment methods

The following table provides a simplified overview of the audit methods associated with each assessment level:

Assessment method	Assessment level 1 (AL 1)	Assessment level 2 (AL 2)	Assessment level 3 (AL 3)
Self-assessment	Yes	Yes	Yes
Evidence	No	Plausibility check	Thorough verification
Interviews	No	Via web conference ^[9]	In person, on site
On-site inspection	No	At your request	Yes

Table 7. Applicability of assessment methods to different assessment levels

Additional information:

- Difference between AL 2 and AL 3
 Methodologically, the two approaches differ significantly. For assessments in assessment level 2, the auditor won't verify anything. He will only check the plausibility. Therefore, the audit provider can't use the results of an assessment in assessment level 2 as a basis for an upgrade to assessment level 3. The efforts for an upgrade to assessment level 3 are essentially the same as for a new initial assessment.
- Plausibility check vs. verification
 Oversimplified, a plausibility check is checking for whether something exists and *looks* right. In contrast, a verification means really checking that something is what it claims to be.
- Information classification and protection needs
 The mapping of information classification (such as confidential or secret) to protection needs can be different for various partners. Therefore, as much as we would like to, we can't provide you a simple table where the information classification of your partner exactly maps to a protection need.

- **Just knowing an assessment level is not enough**

Some partners may request you to get TISAX-assessed with a certain assessment level. Please understand that just knowing the assessment level is not sufficient to start the TISAX process. An assessment level only makes sense in combination with an ISA criteria catalogue and a corresponding protection need. Usually, partners request you to achieve a TISAX label (criteria catalogue plus protection need). However, as protection needs map 1:1 to assessment levels, it is sufficient if you know the criteria catalogue(s) plus the assessment level.

- **Assessment level hierarchy**

Higher assessment levels always include lower assessment levels. For example, if your assessment is based on assessment level 3, it will automatically fulfil all requests for assessment level 2.

- **Our recommendation regarding assessment levels**

If you have to select an assessment objective (and thus implicitly a corresponding assessment level) based on your own judgement, we recommend selecting assessment objectives that imply an assessment level 3. The efforts for TISAX assessments in assessment level 3 are not generally higher than those in assessment level 2.

Suppliers that have several partners often select assessment objectives that imply an assessment level 3. In this way, they are prepared for all future requests and don't have to bother with different assessment levels.

- **Further commercial considerations**

Regarding assessment levels, the total cost of a TISAX assessment consists of the sum of your internal efforts and the cost of the assessment. While the cost of an assessment in assessment level 2 is lower, your internal efforts may be higher. This is due to the fact that an assessment in assessment level 2 usually requires a more comprehensive self-assessment and a better internal documentation. For assessments in assessment level 3, demonstrating how you do things and showing a basic documentation is often sufficient evidence for the auditor. But without an on-site inspection, the auditor will request precise documentation. Therefore, choosing assessment level 3 over assessment level 2 is not uncommon. But it is a choice made by smaller rather than larger companies.

4.3.3.7. Assessment objectives and your own suppliers

TISAX does not necessarily require you to subject all of your own suppliers to the same requirements. If your assessment objective is "Information security with very high protection needs", this does NOT automatically mean that your own suppliers have to achieve the same assessment objective. It does not even mean they need to have TISAX labels at all.

But you still have to check for all of your suppliers whether using their services increases risks or introduces new risks.

Two very simplified examples:


1. You have a policy that regular email can't be used for data with very high protection needs. Therefore, your email provider does not need to achieve the TISAX label with very high protection needs.
You could come to a similar conclusion if you send only encrypted emails and the email provider can't see any of the data with very high protection needs.
2. You dispose of printed data with very high protection needs in the shredder. In such a case, of course, the waste disposal service provider does not have to meet the same requirements as you.

However, the risk assessment may show that your supplier also has to meet the requirements for very high protection needs. In this case, TISAX labels are an option to prove this to you accordingly.


4.3.4. Fee

We raise a fee. Our price list informs you about applicable fees, possible discounts and our payment terms.

You can download the price list on our website at:

 enx.com/en-US/TISAX/downloads/

Direct PDF download:

 enx.com/pricelist.pdf

There are some invoice-related aspects you should consider during your registration preparations:

- Invoice address selection

By default, we will send the invoice to the address you provided as your participant location. But you have the option of providing a different address for receiving the invoice.



Important note:

Please make sure that the invoice address is correct. Accounting laws require that the address on our invoice exactly matches your company's (invoice) address. For compliance reasons, we can't change an invoice address once we issued the invoice.

- Order reference

If you need to see a specific purchase order number or something similar on our invoice, then you have the option to provide us an order reference.

- VAT number

All our charges are subject to German value added tax (VAT) if applicable.

We need this number for processing payments from the EU. It is mandatory to provide a VAT number, if your invoice address is in one of the following countries:

Austria, Belgium, Bulgaria, Croatia, Cyprus (Greek part), Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, United Kingdom

- Supplier management



Important note:

Please understand that due to the mutuality between all TISAX participants, we can't accept any additional terms (such as general purchasing terms, codes of conduct).

Additional information about our invoicing process:

- We can't accept individual purchasing terms.
- We accept:
 - money transfers into the bank account specified on the invoice
 - credit card payments (during the registration process via our payment service provider "[Stripe](https://stripe.com)" (<https://stripe.com>))
- Our invoice will contain the following references to your registration:
 - The name and email address of your main participant contact
 - The assessment scope name

You can find an example invoice in the appendix in Section 7.1, "Annex: Example invoice".

- We provide most facts you would typically require for processing our invoice directly on it. These and even more facts are available in our document "Information for Members and Business Partners". Send us an email and we send you a current version.



Please note:

We are aware that sometimes a company's internal payment approval process is rather lengthy. Therefore, your immediate next step in the TISAX process does not depend on us receiving the payment. But please be aware that you can't share your assessment result if we haven't received your payment.

For this reason, we recommend you ensure that we send our invoice to the appropriate recipient and that it contains an order reference if applicable. You may also want to track internally whether someone paid the invoice.



Important note:

We — ENX Association — invoice the fee. It is only a part of the total cost of a TISAX assessment. Your TISAX audit provider invoices the costs for the assessment(s).

For more information on audit provider-related costs, you may want to refer to Section 5.3.4, "Evaluating offers".



Important note:

The fee is due regardless whether you:

- continue the TISAX process or not.
- successfully pass the TISAX assessment process.

Therefore, the invoice may arrive before you've started the initial assessment.

4.4. ENX portal

The next section will describe the online registration process where you enter all the data you gathered as advised in the previous section. Before you start the online registration process, please let us briefly explain the purpose and benefits of the ENX portal.

The ENX portal allows us to maintain a database of all TISAX participants and it plays an important role throughout the entire TISAX process. During the TISAX registration you enter your data which the TISAX audit providers can then use (if you agree) to calculate their offers and to plan the assessment procedures. Once you go through the TISAX assessment process, you will use the exchange platform on the ENX portal to share your assessment result with your partner.

The portal's name is "ENX portal" instead of "TISAX portal", because we also use the portal to manage other business activities (like the [ENX network](https://enx.com/enxnetwork/) (<https://enx.com/enxnetwork/>)).

4.5. Online registration process

If you prepared according to our advice above (Section 4.3, "Registration preparation"), you are ready to start the online registration process.

4.5.1. Time required

How long it will take you depends heavily on the number of scopes and locations you register. For your first registration as a participant with one scope with one location, you should expect a minimum time of 20 minutes.

We recommend completing the registration in a single session, because currently you can't easily catch up some steps later. Should you still need to pause, we will contact you to request any missing data.

4.5.2. Start here

Please start your registration on our website at:

enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

Basically, all you need to do is follow the on-screen instructions. Nevertheless, we briefly describe the process below.

4.5.3. Portal account

Your first step is to create an account for yourself in the ENX portal. You need the portal account to be able to manage your company's "participant data".



Please note:

Should the ENX portal claim that your email address is already in use, please contact us. This message may indicate that for some reason you are already stored in our system.



Please note:

As described, portal accounts are not necessarily "participant contacts" or "scope contacts" (see below) with an active role in the assessment process.

Vice versa, a "participant contact" or "scope contact" doesn't automatically include the same rights to manage the participant data as with a portal account. This means, colleagues named as "participant contact" or "scope contact" can't automatically access the participant data in the ENX portal.

If you want to assign the right to manage the participant data to a contact who you already created in the ENX portal (regardless whether you assigned him a role), you need to invite the contact. For more information, please refer to last note in Section 4.5.5, "Participant contact".

4.5.4. Participant registration

Your second step is to register your company as a TISAX participant. The "TISAX participant" is the company that exchanges assessment results with other participants.

4.5.5. Participant contact

This is the person that is generally responsible for all information security assessment topics of your company. This can be either you or someone else in your company.

The main participant contact is usually all we need. Should you prefer to have all communication sent by us and our TISAX audit providers in the context of this registration also to other persons as well, please add additional participant contacts.



Important note:

We recommend assigning at least one alternate for each contact. If a contact is temporarily unavailable or leaves the company, someone else can manage your company's participant data. If you need to assign a new contact (without any other remaining valid contacts), you have to go through a complex process. Our process ensures that only persons who can prove that they are entitled to legally represent the company can approve assigning a new main contact.



Please note:

You can always add or remove contacts at a later point in time (even after completing the online registration process and even once you completed assessments).



Please note:

You can't use group email addresses for participant contacts (like "info@acme.com" or "IT@acme.com").

This is in line with the ISA requirements regarding user logins.



Please note:

You can choose if each contact should have access to your company's participant data. Either:

1. You just add the contact. The contact is stored in our system, but can't login and manage any data.
2. Or you invite the contact. Then the ENX portal sends an invitation email to the contact. The contact must follow the invitation link in the email. Once the contact has created his own personal account for the ENX portal, he can manage your company's participant data.

To create a new contact: Sign in > MY TISAX > ADMINISTRATORS > Create new TISAX Administrator

To invite a contact: Sign in > MY TISAX > ADMINISTRATORS > Go to the end of the table row of the contact and click the button with the down arrow > Edit TISAX Administrator > Go to the section "ENX PORTAL ACCESS" > Set "INVITE THIS CONTACT" to "Yes" > Click "Save Contact"

4.5.6. General Terms and Conditions

Your third step is to accept the "TISAX Participation General Terms and Conditions".

You may want to refer back to the explanatory notes in Section 4.3.1, "The legal foundation".

4.5.7. Assessment scope registration

Your fourth step is to register the assessment scope of your information security assessment.

We ask you to:

- assign an assessment scope name.
The main purpose of the scope name is to make it easy for you to identify a scope in the overview list of scopes in the ENX portal.
You may want to refer back to the explanatory notes in Section 4.3.2.6, "Scope name"
- choose an assessment scope type.
(Standard, Custom)
You may want to refer back to the explanatory notes in Section 4.3.2, "The TISAX assessment scope".
- specify the main scope contact.
This is the person who is generally responsible for the assessment of a particular scope. This can be either you or someone else in your company.
The main scope contact is usually all we need. Should you prefer to have all communication sent by us in the context of this particular scope also to other persons, you can add additional participant contacts.

- select your assessment objective(s).

You may want to refer back to the explanatory notes in Section 4.3.3, “Assessment objectives”.

- add assessment scope location(s).

We request that you specify all locations that are part of the assessment scope.

You may want to refer back to the explanatory notes in Section 4.3.2, “The TISAX assessment scope”.



Please note:

Once you created a new location, you can't edit it. For minor changes (change of company name, typos in street name, postal code, city, etc.), please contact us. We will do the editing for you.



Important note:

This note is only relevant if you are renewing your TISAX labels.

Please reuse the existing location records that you created and used during the registration of your previous scope. Don't create a new location record with the same address.

The reason for this: Some TISAX participants process the assessment results of their partners automatically. They synchronise their own system with the ENX portal. Even tiny differences may block the successful synchronisation. Besides that, you don't clutter your participant data with unnecessary duplicates.

- select publication and sharing levels (optional).

You can already decide to publish your assessment result to other TISAX participants and to share your assessment result with your partner(s). Typically, you would be allowing us to at least show that your company is a participant and that you successfully passed the TISAX process.

You can safely skip this step during your initial registration. You can always define access to your assessment result later.

You may want to refer back to the explanatory notes in Section 4.3.2.8, “Publication and sharing”.



Important note:

You can't revoke any publication or sharing permissions.

For details, please refer to Section 6.4, “Permanence of exchanged results”.

- specify who receives the invoice.

We request that you specify who will receive our invoice(s).

You may want to refer back to the explanatory notes in Section 4.3.4, “Fee”.



Please note:

You can't do much wrong here. If you later find out that you should have registered a slightly different scope (you forgot a location, you have another assessment objective, etc.), the audit provider can nevertheless conduct the assessment.

Example: The auditor determines that the scope must contain an additional location that you originally didn't add to the scope. The auditor will proceed and afterwards updates your assessment scope in the ENX portal while uploading your assessment result.



Please note:

Every assessment scope goes through a lifecycle. At this stage, your assessment scope either has the status “Incomplete”, “Awaiting your order” or “Awaiting ENX approval”.

For more information on the status of an assessment scope, please refer to Section 7.5.1, “Overview: Assessment scope status”.



Please note:


For large corporations with many locations, TISAX offers the simplified group assessment. You can consider this option if:

- you have at least three locations in your scope^[10] and
- your information security management system is in top form and centrally organised^[11].

For a simplified group assessment the initial effort is higher. However, this pays off the more locations you have.

For more information on the “simplified group assessment”, please refer to the document “TISAX Simplified Group Assessment”.

You can download the document “TISAX Simplified Group Assessment” on our website at:

 enx.com/en-US/TISAX/downloads/

Direct PDF download:

 enx.com/sga.pdf



Please note:

Once we have registered your assessment scope, you can't change it yourself.

If you can credibly assure us that you have NOT yet sent your “TISAX scope excerpt” to our audit providers, please contact us. We can change it for you.

If you already sent your “TISAX scope excerpt” to (one of) our audit providers, you just create the new location(s) in the ENX portal (if applicable) and discuss any changes with your audit provider. Your audit provider will conduct the assessment based on the changes and update the scope information in the ENX portal.



Please note:

It is not possible for you to delete an assessment scope in the ENX portal. If you created an assessment scope by mistake, please contact us. We will delete it for you.

4.5.8. Confirmation email

Once you completed all of the mandatory steps above, we will check your application. We will then send you a confirmation email.

This email has two important elements:

- A contact list of all TISAX audit providers

You must choose one of our TISAX audit providers to conduct an assessment of your assessment scope. You can use the contacts to request offers.

For more information on audit provider selection, please refer to Section 5.3, “Audit provider selection”.

- The “TISAX Scope Excerpt” as an attached PDF file

It contains:

- The information that we stored in our database
- Your Participant ID
Please refer to Section 4.5.8.1, “Participant ID” below.
- Your Scope ID(s)
Please refer to Section 4.5.8.2, “Scope ID” below.

For an example of our confirmation email, please refer to Section 7.2, “Annex: Example confirmation email”.

For an example of the “TISAX Scope Excerpt”, please refer to Section 7.3, “Annex: Example TISAX Scope Excerpt”.

You will receive our confirmation email usually within three business days.

If you don’t hear from us within seven business days, please verify that a) you provided all information and b) the assessment scope status is “Awaiting ENX approval”. We will start processing your registration only when everything is complete. If you think everything is complete but we haven’t contacted you, please contact us.

We send our confirmation email to the main participant contact.



Please note:

Every assessment scope goes through a life cycle. At this stage, your assessment scope has the status “Awaiting ENX approval”.

For more information on the status of an assessment scope, please refer to Section 7.5.5, “Assessment scope status “Awaiting your payment””.

The next two sub-sections provide detailed information about the purpose of your Participant ID and the Scope ID.

4.5.8.1. Participant ID

The Participant ID:

- identifies a TISAX participant.
- is unique for each participant.
- is assigned by us upon completion of the registration.
- is a prerequisite for ordering an information security assessment by any of our TISAX audit providers.
- looks like this:

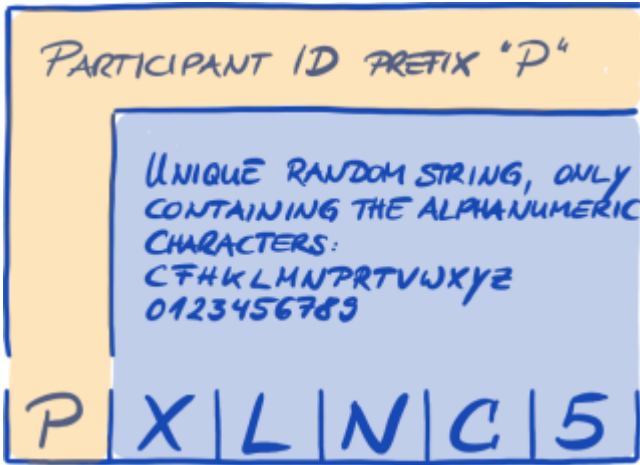


Figure 9. Format of the Participant ID^[12]



Please note:

There are two ways to find your Participant ID:

1. Check your "TISAX Scope Excerpt".

Please refer to Section 4.5.8, "Confirmation email" above.

2. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/), go to the main navigation bar and select "DASHBOARD". There you will find your Participant ID.

4.5.8.2. Scope ID

The Scope ID:

- identifies an assessment scope.
- is unique for each assessment scope.
- is assigned by us upon completion of the registration.
- is a prerequisite for being allowed to order an information security assessment by any of our TISAX audit providers.
- looks like this:

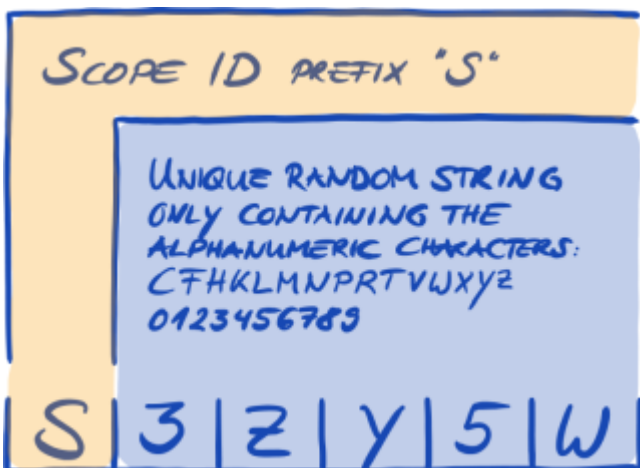


Figure 10. Format of the Scope ID



Please note:

There are two ways to find your Scope ID:

1. Check your “TISAX Scope Excerpt”.

Please refer to Section 4.5.8, “Confirmation email” above.

2. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (<https://enx.com/en-US/TISAX/>), go to the main navigation bar, select “MY TISAX” and then “SCOPES AND ASSESSMENTS”. There you will find your Scope ID(s).



Please note:

Every assessment scope (identified by its Scope ID) runs through a life cycle.

For more information on the status of an assessment scope, please refer to Section 7.5, “Annex: Assessment scope status”.

4.5.9. Status information

At this stage, there are two relevant statuses that we use to describe your position in the TISAX process:

1. Participant status
2. Assessment scope status

The following diagram illustrates the conditions that must be met to reach a certain status:

- YOUR ACTIONS
- OUR ACTIONS

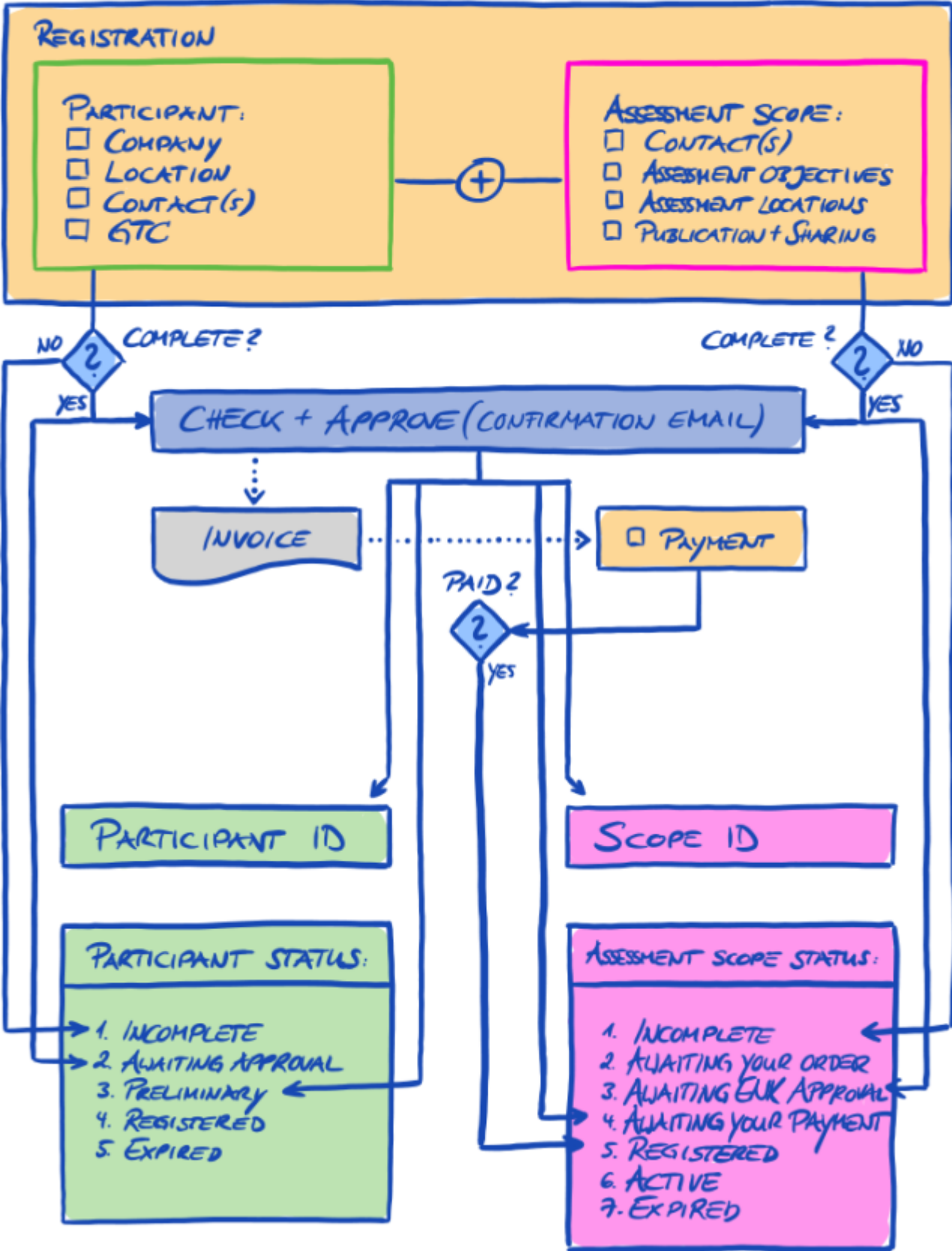


Figure 11. Conditions for the participant status and assessment scope status

You can find the status definitions and what you need to do to progress to the next status in the annex.

For more information on the:

- participant status, please refer to Section 7.4, “Annex: Participant status”.
- assessment scope status, please refer to Section 7.5, “Annex: Assessment scope status”.

4.5.10. Changes of your registration information



Please note:

For all answers regarding the data life cycle, please refer to Section 7.9, “Annex: Participant data life cycle management”. It contains instructions for cases where you want to change or update data such as your company name or your contact information.

Congratulations, you are now a registered TISAX participant. You are ready to continue with the next step in the TISAX process.

5. Assessment (Step 2)

The estimated reading time for the assessment section is 30-35 minutes.

5.1. Overview

The TISAX assessment is your second step. This is where you do most of the work of getting TISAX-assessed.

The following sections will guide you through the assessment:

1. We start with explaining how you can use the ISA self-assessment to find out whether you are prepared for a TISAX assessment.
2. Then we advise you how to choose one of our TISAX audit providers.
3. Next, we describe your way through the assessment process.
4. At the end, we explain the “process outcome”: your assessment result and the associated TISAX labels.

5.2. Self-assessment based on the 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 ISA.

The “Information Security Assessment” (ISA) is a criteria catalogue published by the “German Association of the Automotive Industry” (Verband der Automobilindustrie e.V. - VDA). It is the automotive industry’s standard for information security assessments.

The following sections focus on practical instructions for conducting a self-assessment based on the ISA.

The explanations, examples and screenshots in this handbook are based on Version 5 of the ISA.



Please note:

You will find information on changes compared with previous versions of the ISA in its Excel sheet “Change history”.



Please note:

For information about which ISA version is applicable to your assessment when the VDA publishes a new version, please refer to Section 7.11, “Annex: ISA life cycle management”.

5.2.1. Download the ISA document

Start your self-assessment by downloading the ISA document.

You can download it from our website at:

enx.com/en-US/TISAX/downloads/

Direct Excel file download:

portal.enx.com/isa5-en.xlsx

The ISA document is also available in German:

enx.com/de-de/TISAX/downloads/

5.2.2. Understand the ISA document

Before you start your self-assessment, here are some explanations you may find useful. We provide these in addition to the official explanations and definitions in the ISA document, but with a focus on use for TISAX assessments.

5.2.2.1. Criteria catalogues

The ISA currently has three “criteria catalogues”^[13]:

1.	Information Security
2.	Prototype Protection
3.	Data Protection

Each criteria catalogue has its own Excel sheet:



Figure 12. Screenshot: ISA criteria catalogues as Excel sheets

The core of the ISA is the criteria catalogue “Information Security”. The questions in this criteria catalogue are mandatory for all TISAX assessments.

The other criteria catalogues are optional. Their applicability depends on your assessment objective(s).

The aforementioned assessment objectives map to these criteria catalogues:

No.	Assessment objective	ISA criteria catalogue
1.	Handling of information with high protection needs	Information Security
2.	Handling of information with <u>very</u> high protection needs	Information Security
3.	Protection of prototype parts and components	Prototype Protection

No.	Assessment objective	ISA criteria catalogue
4.	Protection of prototype vehicles	Prototype Protection
5.	Handling of test vehicles	Prototype Protection
6.	Protection of prototypes during events and film or photo shoots	Prototype Protection
7.	Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	Data Protection
8.	Data protection with <u>special</u> categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	Data Protection

Table 8. Mapping between TISAX assessment objectives and ISA criteria catalogues

Example: If you have selected the assessment objective “Data Protection”, then you will have to answer the questions in the criteria catalogues “Information Security” AND “Data Protection”.

You may have noticed that there is more than one assessment objective per criteria catalogue. How do you know which requirements are applicable to which assessment objective?

The following table shows you which requirements are applicable:

No.	Assessment objective	Applicable requirements
1.	Handling of information with high protection needs	<ul style="list-style-type: none"> ▪ All requirements from the criteria catalogue “Information Security” (columns “Requirements (must)” and “Requirements (should)”) <ul style="list-style-type: none"> ▪ Plus the additional requirements in the column “Additional requirements for high protection needs” (if applicable)
2.	Handling of information with <u>very</u> high protection needs	<ul style="list-style-type: none"> ▪ All requirements from the criteria catalogue “Information Security” (columns “Requirements (must)” and “Requirements (should)”) <ul style="list-style-type: none"> ▪ Plus the additional requirements in the columns “Additional requirements for high protection needs” and “Additional requirements for <u>very</u> high protection needs” (if applicable)
3.	Protection of prototype parts and components	<ul style="list-style-type: none"> ▪ All requirements applicable to the assessment objective “Handling of information with high protection needs” ▪ Plus the requirements in the following chapters of the criteria catalogue “Prototype Protection”: <ul style="list-style-type: none"> ▪ 8.1 Physical and Environmental Security ▪ 8.2 Organizational Requirements ▪ 8.3 Handling of vehicles, components and parts

No.	Assessment objective	Applicable requirements
4.	Protection of prototype vehicles	<ul style="list-style-type: none"> ▪ All requirements applicable to the assessment objective “Handling of information with high protection needs” ▪ Plus the requirements in the following chapters of the criteria catalogue “Prototype Protection”: <ul style="list-style-type: none"> ▪ 8.1 Physical and Environmental Security ▪ 8.2 Organizational Requirements ▪ 8.3 Handling of vehicles, components and parts ▪ Plus the additional requirements in the column “Additional requirements for vehicles classified as requiring protection” (if applicable)
5.	Handling of test vehicles	<ul style="list-style-type: none"> ▪ All requirements applicable to the assessment objective “Handling of information with high protection needs” ▪ Plus the requirements in the following chapters of the criteria catalogue “Prototype Protection”: <ul style="list-style-type: none"> ▪ 8.2 Organizational Requirements ▪ 8.3 Handling of vehicles, components and parts ▪ 8.4 Requirements for trial vehicles
6.	Protection of prototypes during events and film or photo shoots	<ul style="list-style-type: none"> ▪ All requirements applicable to the assessment objective “Handling of information with high protection needs” ▪ Plus the requirements in the following chapters of the criteria catalogue “Prototype Protection”: <ul style="list-style-type: none"> ▪ 8.2 Organizational Requirements ▪ 8.3 Handling of vehicles, components and parts ▪ 8.5 Requirements for events and shootings
7.	Data protection	<ul style="list-style-type: none"> ▪ All requirements applicable to the assessment objective “Handling of information with high protection needs” ▪ All requirements from the criteria catalogue “Data Protection”
8.	Data protection with <u>special</u> categories of personal data	<ul style="list-style-type: none"> ▪ All requirements applicable to the assessment objective “Handling of information with <u>very</u> high protection needs” ▪ All requirements from the criteria catalogue “Data Protection”

Table 9. Applicability of requirements to the assessment objectives

The screenshot below shows the main elements of the questions in each criteria catalogue. We explain all elements further down.

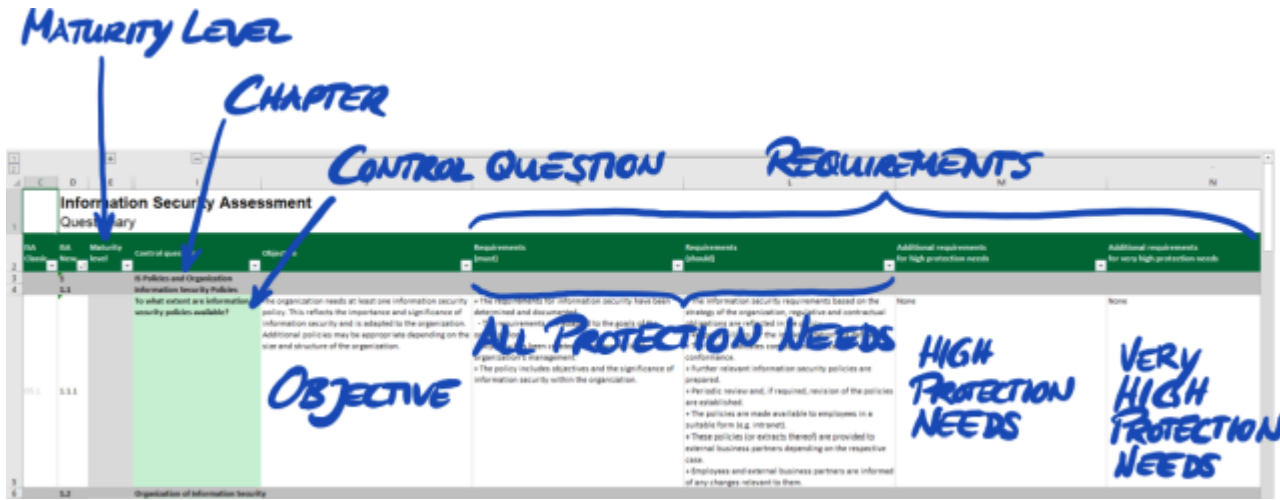


Figure 13. Screenshot: Main elements of the questions in the ISA criteria catalogues

5.2.2.2. Chapters

Each criteria catalogue groups the questions in chapters.

Example: “2 Human Resources”

The grouping is based on the typical responsibilities in a company. These departments are specified in the column “Usual person responsible for process implementation” (“HR” in the example above).

5.2.2.3. Control questions

You find the questions for each criteria catalogue in the respective Excel sheets.

Example: “4.1.2 To what extent is the user access to network services, IT systems and IT applications secured?”

The control questions are also referred to as “controls”. This is “auditor speak”. The ISO standards that the ISA builds upon use the term “control”.

5.2.2.4. Self-assessment form fields

Between the columns “Maturity level” and “Control question” are form fields you need to fill in when you are conducting a self-assessment:

Form field	Purpose	Mandatory?
Implementation description (Column F)	Here you should briefly describe what you implemented to address this control question in your company.	Yes
Reference Documentation (Column G)	Here you should specify in which document(s) you prove the implementation.	Yes
Findings/Result (Column H)	Here you can write down any findings where you think a gap exists between what should be and what is.	No

Table 10. Self-assessment form fields and their purpose

Only the brief description of your implementation and the reference to your documentation are mandatory. This information will help our TISAX audit providers to better understand your company and to prepare the assessment.

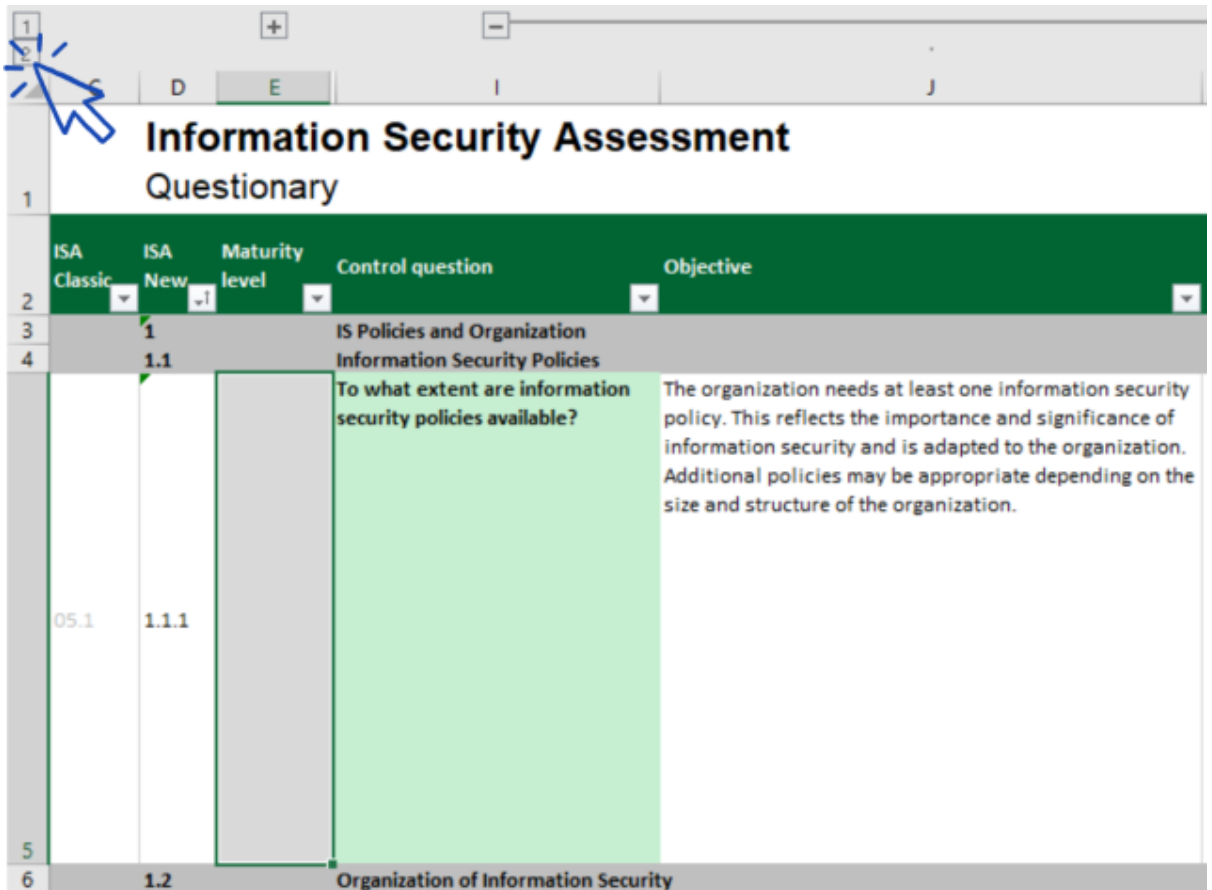
There are more optional columns to support your self-assessment:

- Measures/recommendations (Column R)
- Date of assessment (Column S)
- Date of completion (Column T)
- Responsible department (Column U)
- Contact (Column V)



Important note:

If you open the downloaded Excel file and select one of the criteria catalogue worksheets (e.g. Information Security), you probably won't immediately see the self-assessment form fields. To show them, you need to click on the grouping button for level "2"^[14]. The button is above and to the left of cell C1. This will expand the view to show the self-assessment form fields.



Another tip is to use the arrow keys to scroll down. Because due to the large size of the cells, the scrolling with the scroll bar may require excellent fine motor skills. If you use your pointing device's scroll feature, you may also accidentally skip over some of the larger cells.

5.2.2.5. Objective

To the right of the column "Control question" is the column "Objective" (column J). Its content describes what you need to achieve regarding this aspect of your information security management.

Example (for control question 4.1.2): "Only securely identified (authenticated) users are to gain access to IT systems. For this purpose, the identity of a user is securely determined by suitable procedures."

5.2.2.6. Requirements

The requirements are what you are expected to fulfil in order to achieve the objective.

The requirements are spread across four columns:

1. Requirements (must) (Column K)
2. Requirements (should) (Column L)
3. Additional requirements for high protection needs (Column M)
4. Additional requirements for very high protection needs (Column N)

You have to fulfil all requirements up to the protection need you need to achieve (which you can derive from your assessment objective).

For more information about the ISA definitions of the requirement levels “must” and “should”, please refer to the “Key terms” in the Excel sheet “Definitions”.



Important note:

It is very important for you to understand that you have to interpret each requirement in the context and spirit of the objective. Even fulfilling a requirement to the letter doesn't guarantee that the audit provider confirms that you fulfil it in the context and spirit of the objective (column J).

The requirements and their wording are based on a theoretical implementation by a fictional average company of unknown size.

The audit provider has to always weigh the objective against the unique implementation at your company. What is appropriate for the average company might not be sufficient in your particular situation.

For more information, please refer to Section 5.2.5, “Address the self-assessment result”.

5.2.2.7. Maturity levels

The ISA uses the concept of “maturity levels” to rate the quality of all aspects of your information security management system. The more sophisticated your information security management system is, the higher your maturity level will be.

The ISA differentiates six maturity levels. You can find the detailed definition in the Excel sheet “Maturity levels”. For a consolidated view on the maturity levels, we quote the informal descriptions as provided in the ISA:

Maturity level	In one word	Description
0	Incomplete	A process is not available, not followed or not suitable for achieving the objective.
1	Performed	An undocumented or incompletely documented process is followed and indicators exist that it achieves its objective.
2	Managed	A process achieving its objectives is followed. Process documentation and process implementation evidence are available.

Maturity level	In one word	Description
3	Established	A standard process integrated into the overall system is followed. Dependencies on other processes are documented and suitable interfaces are created. Evidence exists that the process has been used sustainably and actively over an extended period.
4	Predictable	An established process is followed. The effectiveness of the process is continually monitored by collecting key figures. Limit values are defined at which the process is considered to be insufficiently effective and requires adjustment. (Key Performance Indicators)
5	Optimizing	A predictable process with continual improvement as a major objective is followed. Improvement is actively advanced by dedicated resources.

Table 11. Informal description of the maturity levels

You have to rate the maturity level of your information security management system per question. Enter your maturity level in the column “Maturity level” (column E).

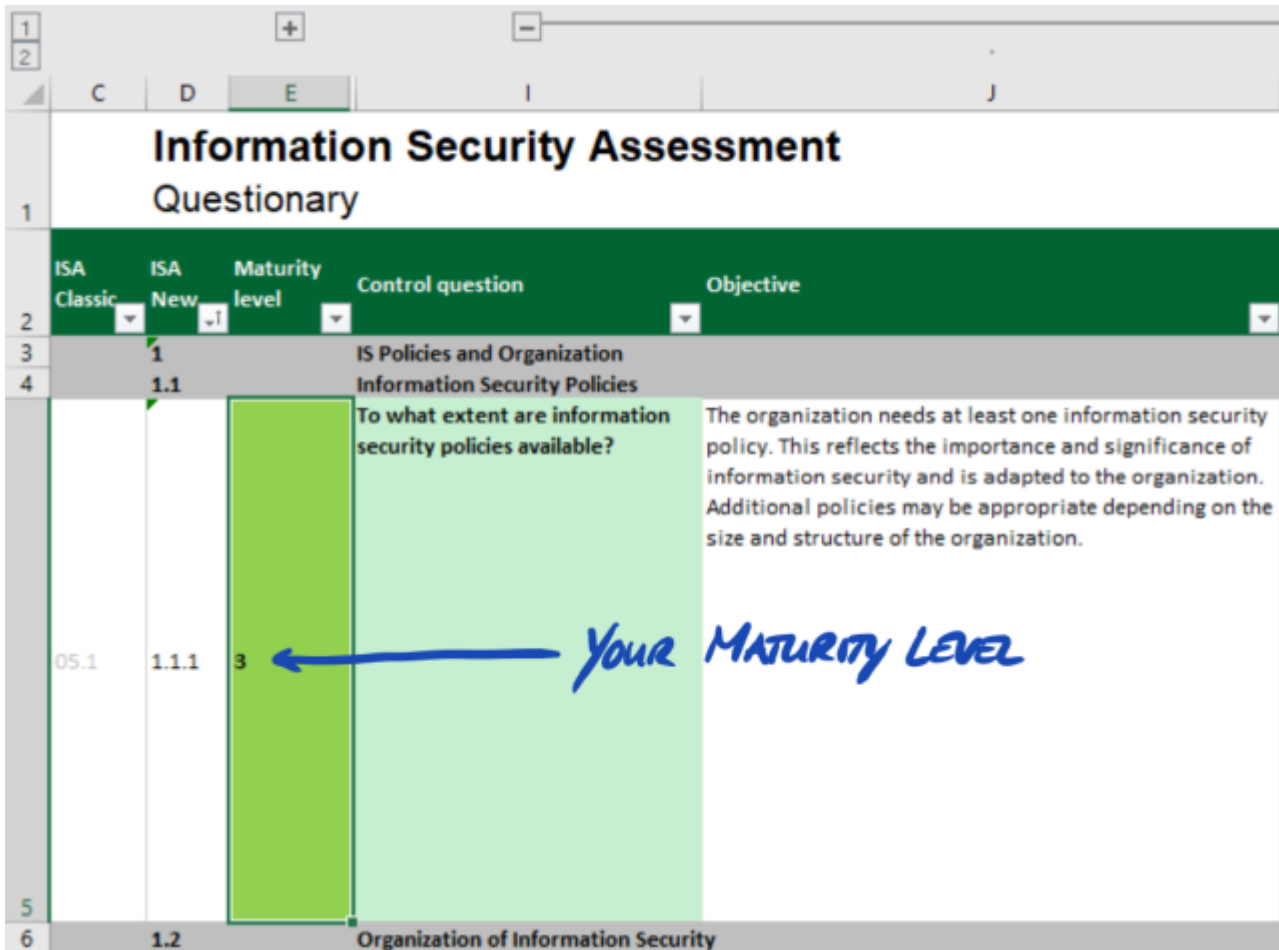


Figure 14. Screenshot: Example of maturity level selection in the ISA document (Excel sheet “Information Security”)

For more information on target maturity levels and their impact on your assessment result, please refer to Section 5.2.4, “Interpret the self-assessment result”.

With this improved understanding, you are now ready to start the self-assessment.

5.2.3. Conduct the self-assessment

Open the Excel file and go through all the control questions of each criteria catalogue applicable to your assessment objective(s) and determine the maturity level that matches the current state of your information security management system. Do this based on your own best judgement. There is no right or wrong at this stage.

Once you completed the self-assessment, the “Result” column (H) in the Excel sheet “Results (ISA5)” should be completely filled, either with numbers (0-5) or “n.a.” (as in “not applicable”).

No.	Subject	target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

GREEN = ✓

Figure 15. Screenshot: Example of “Results (ISA5)” sheet in the ISA document

If you have questions regarding the ISA, please contact us.

5.2.4. Interpret the self-assessment result

The next five sub-sections explain how to analyse and interpret your self-assessment result. The analysis will tell you whether you are ready or not yet ready for a TISAX assessment.

5.2.4.1. Analysis

Your result score summarises the self-assessment result.

You find the result score (“Result with cutback to target maturity level”) in the Excel sheet “Results (ISA5)” (cell D6). We will explain “cutback” soon.

Information Security Assessment Results



Result with cutback to target maturity level: 3,00		Maximum score: 3,00	
Details: YOUR RESULT SCORE		MAXIMUM RESULT SCORE	
No.	Subject	target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figure 16. Screenshot: Your result score and the maximum result score (Excel sheet "Results (ISA5)", cell D6 and G6)

For understanding and subsequently interpreting your self-assessment result and your result score, you need to differentiate two analysis levels:

1. **Question level**

This level has all the questions. For each question, there is a target maturity level and your maturity level.

2. **Score level**

On this level, there is the overall result that summarises the results of all the questions. There is a maximum result score and your result score.

The figure below shows the analysis levels:

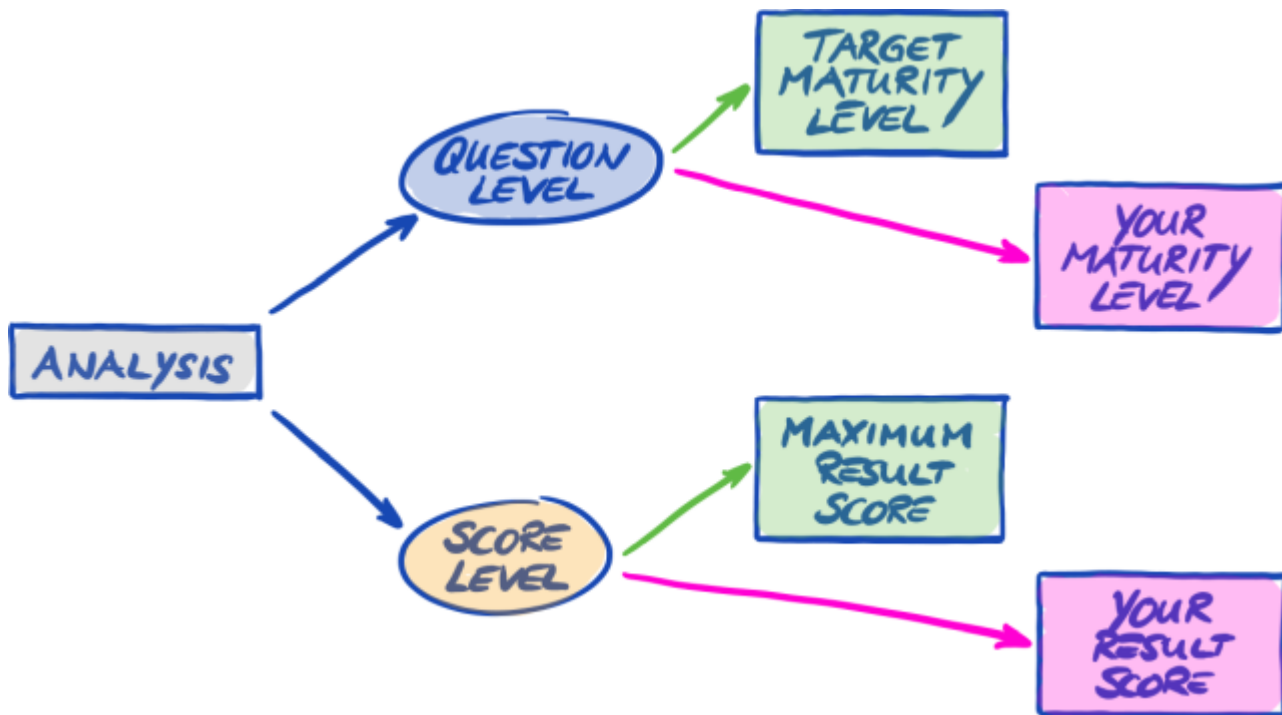


Figure 17. Analysis of the self-assessment result on the question level and the score level

The figure below shows you where to find the results on the **score level** and the results on the **question level**:

Information Security Assessment

Results **SCORE LEVEL** ↔



Result with cutback to target maturity level: 3,00	Maximum score: 3,00
----------------------------------------------------	---------------------

Details:

No.	Subject	QUESTION LEVEL	target maturity level	Result
1.1.1	To what extent are information security policies available?		3	3
1.2.1	To what extent is information security managed within the organization?		3	3
1.2.2	To what extent are information security responsibilities organized?		3	3

Figure 18. Score level and question level in the Excel sheet "Results (ISA5)"

The next figure shows a simplified view of the analysis levels, the ISA target definitions and your own results:

TARGET MATURITY LEVEL

(QUESTION LEVEL)

Q	TML	YML
1.1.1	3	3
1.2.1	3	3
1.2.2	3	3

YOUR MATURITY LEVEL

(QUESTION LEVEL)

Q	TML	YML
1.1.1	3	3
1.2.1	3	3
1.2.2	3	3

MAXIMUM RESULT SCORE

(SCORE LEVEL)

Q	TML	YML
1.1.1	3	3
1.2.1	3	3
1.2.2	3	3
	30	30

YOUR RESULT SCORE

(SCORE LEVEL)

Q	TML	YML
1.1.1	3	3
1.2.1	3	3
1.2.2	3	3
	30	30

Figure 19. The targets and your results on the question level and the score level

The following sections explain the result and its analysis in detail.

5.2.4.2. The target maturity level (on question level)

The ISA defines a “target maturity level” of 3 for each question.

For more information on the definition of each maturity level, please refer to Section 5.2.2, “Understand the ISA document”.

The ISA defines the target maturity levels in the Excel sheet “Results (ISA5)” (starting at column G, row 22; see figure below).

TARGET MATURITY LEVEL →

No.	Subject	target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figure 20. The target maturity level definition in the Excel sheet “Results (ISA5)”

5.2.4.3. Your result (on question level)

In order to receive TISAX labels, you usually need to have maturity levels for each question that are equal to or above the target maturity level.

Example: If the target maturity level for question X is “3”, your maturity level for that question should be “3” or higher. If your maturity level for that question is below “3”, you may not receive TISAX labels.

This has to happen for each question. If the target maturity level for two questions is “3”, you can’t compensate for a maturity level of “2” for one question with a maturity level of “4” for the other question.

The ISA document automatically transfers your maturity levels from the Excel sheet “Information Security” (column E) to the Excel sheet “Results (ISA5)” (starting at column H, row 23):

YOUR MATURITY LEVEL →

No.	Subject	target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figure 21. Your maturity levels in the Excel sheet “Results (ISA5)”

Your maturity level is subject to a calculation before the ISA document summarises it in your result score. Basically, your maturity level is “cut back” to the target maturity level. This is done so that questions where your maturity level is *above* the target maturity level don’t compensate for questions where your maturity level is *below* the target maturity level.

Here’s how the ISA calculates your result on the question level:

- It takes your maturity level and compares it to the question’s target maturity level.
- If your maturity level is above the target maturity level, it is “cut back” to the target maturity level.

- If your maturity level is below or equal to the target maturity level, nothing happens for this question. Example (see figure below): The target maturity level is “3”. Your maturity level is “4”. Your “cut back result” for this question will be “3”.

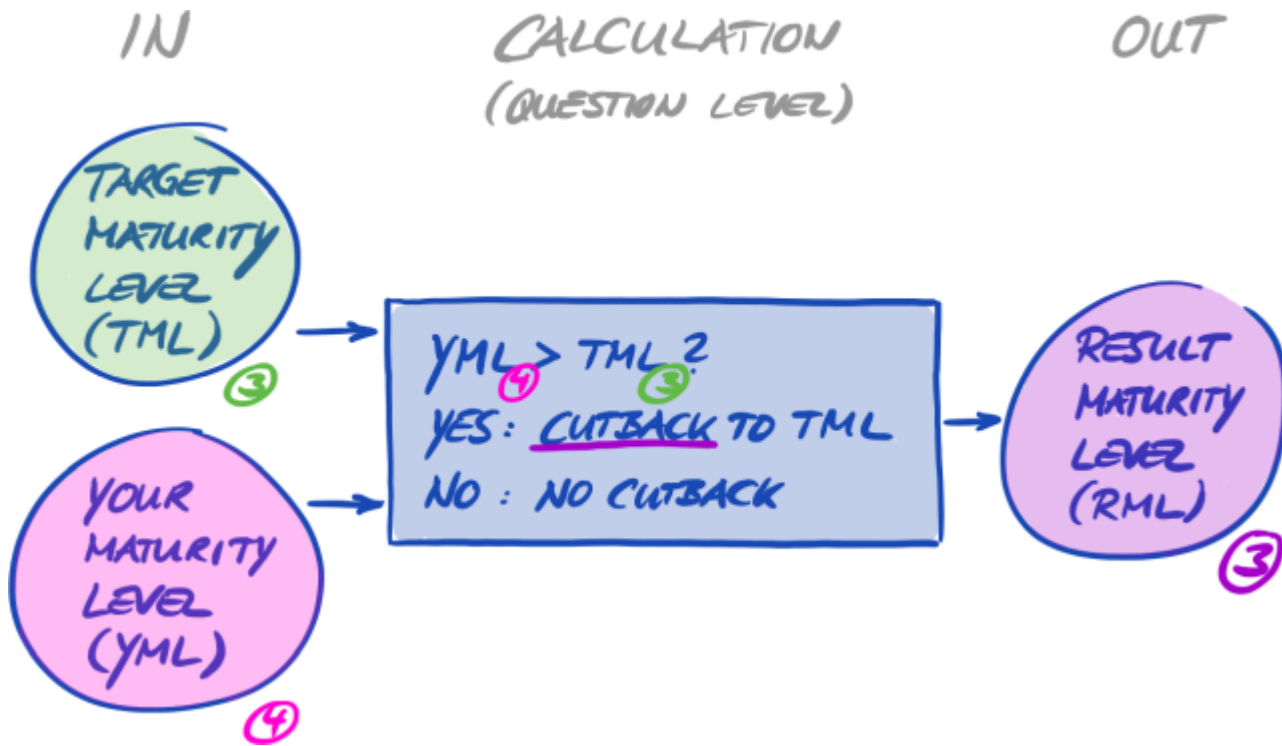


Figure 22. Cutback calculation of the result maturity level

The figure below shows that if your maturity level is higher than the target maturity level, the ISA cuts it back (the colours green, orange and red match with the colours used in the “Result” column, see Figure 21, “Your maturity levels in the Excel sheet “Results (ISA5)”).

EXAMPLE:

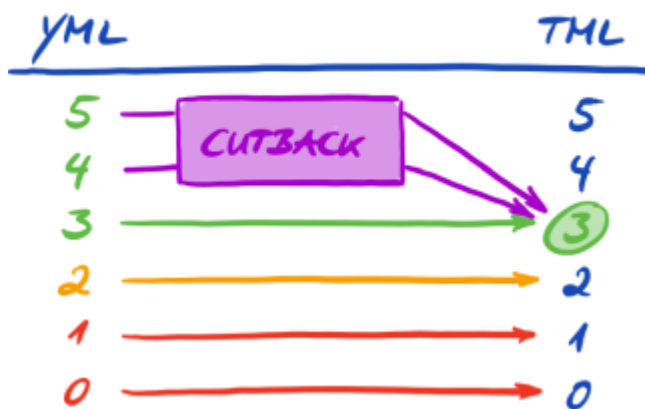


Figure 23. Cutback illustration with the colours used in the Excel sheet “Results (ISA5)”

Below is another way to view the maturity levels on the question level. The colours of the circles illustrate the target maturity level or the “distance” to it (example: the circle is orange if the maturity level is “-1” below the target maturity level). The check marks illustrate your maturity level.

QUESTION	MATURITY LEVEL					
	0	1	2	3	4	5
1.1.1	○	○	○	✓	○	○
1.2.1	○	○	✓	○	○	○
1.2.2	○	✓	○	○	○	○
1.2.3	○	○	○	✓	✓	○

CUTBACK

- TARGET MATURITY LEVEL (TML)
- ONE OR MORE ABOVE THE TML
- ONE BELOW THE TML
- TWO OR MORE BELOW THE TML
- ✓ YOUR MATURITY LEVEL (YML)
- ✓ CUTBACK TO TML

Figure 24. Maturity levels on question level



Please note:

It is possible to successfully pass a TISAX assessment even if you don't reach the target maturity level for all questions. The main question in such cases is whether you have a relevant risk. If your maturity level is below the target value, but there is no risk, this might still be sufficient.

5.2.4.4. The target (on score level)

The ISA defines an "ideal" overall maturity level — the "maximum result score" (or "Maximum score", cell G6).

Information Security Assessment Results



Result with cutback to target maturity level:	3,00	Maximum score:	3,00
-----------------------------------------------	------	----------------	------

MAXIMUM RESULT SCORE

No.	Subject	target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figure 25. Maximum result score (Excel sheet "Results (ISA5)")

In theory, this overall maturity level is the average of all target maturity levels (on the question level). This would be a maximum result score of "3.0".

However, it is "3.0" only if all questions apply to your situation. As soon as a question is not applicable to your situation, the average changes and the maximum result score is lower than "3.0".

Based on a view shown further above (Figure 24, "Maturity levels on question level"), you can see below what's put into the average for the maximum result score:

QUESTION	MATURITY LEVEL						
	0	1	2	3	4	5	
1.1.1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.2.1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.2.2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.2.3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	

CUTBACK

MAXIMUM RESULT SCORE

Figure 26. The maximum result score (on score level)

5.2.4.5. Your result (on score level)

Your overall result score ("Result with cutback to target maturity levels", cell D6):

- summarises the overall maturity level of your information security management system.
- is the average of all your maturity levels (on question level).
- can be below or equal to the maximum result score.
- should be as close to the maximum result score as possible. The more your result score is below the maximum result score, the less likely it is that you will receive TISAX labels.

Information Security Assessment Results



Result with cutback to target maturity level:	3,00	Maximum score:	3,00
-----------------------------------------------	------	----------------	------

Details: **YOUR RESULT SCORE**

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figure 27. Your result score (Excel sheet "Results (ISA5)")

Again using a view shown further above (Figure 24, "Maturity levels on question level"), you can see below what's put into the average for the result score:

QUESTION	MATURITY LEVEL						
	0	1	2	3	4	5	
1.1.1	○	○	○	✓	○	○	
1.2.1	○	○	✓	○	○	○	
1.2.2	○	✓	○	○	○	○	
1.2.3	○	○	○	✓	✓	○	

CUTBACK

YOUR RESULT SCORE

Figure 28. Your result score (on score level)

The result score tells you whether you:

- are ready for a TISAX assessment.
- can expect to receive TISAX labels.

If your result score (“Result with cutback to target maturity levels”) is below “3.0”, then at least for one question your maturity level doesn’t match the target maturity level. In this case, you probably must improve your information security management system before you are ready for your TISAX assessment.



Please note:

For the overall score, there are formal limits for an acceptable “distance” between your result score and the maximum result score (“Result with cutback to target maturity levels”).

If your result score is more than:

- 10% below, the overall assessment result will be “minor non-conform”.
- 30% below, the overall assessment result will be “major non-conform”.



Important note:

Having a result score (“Result with cutback to target maturity levels”) of “3” is not a guarantee that you will pass the TISAX assessment without any prohibitive findings. Please bear in mind that the audit provider may view certain aspects differently than you do.

5.2.4.6. Are you ready?

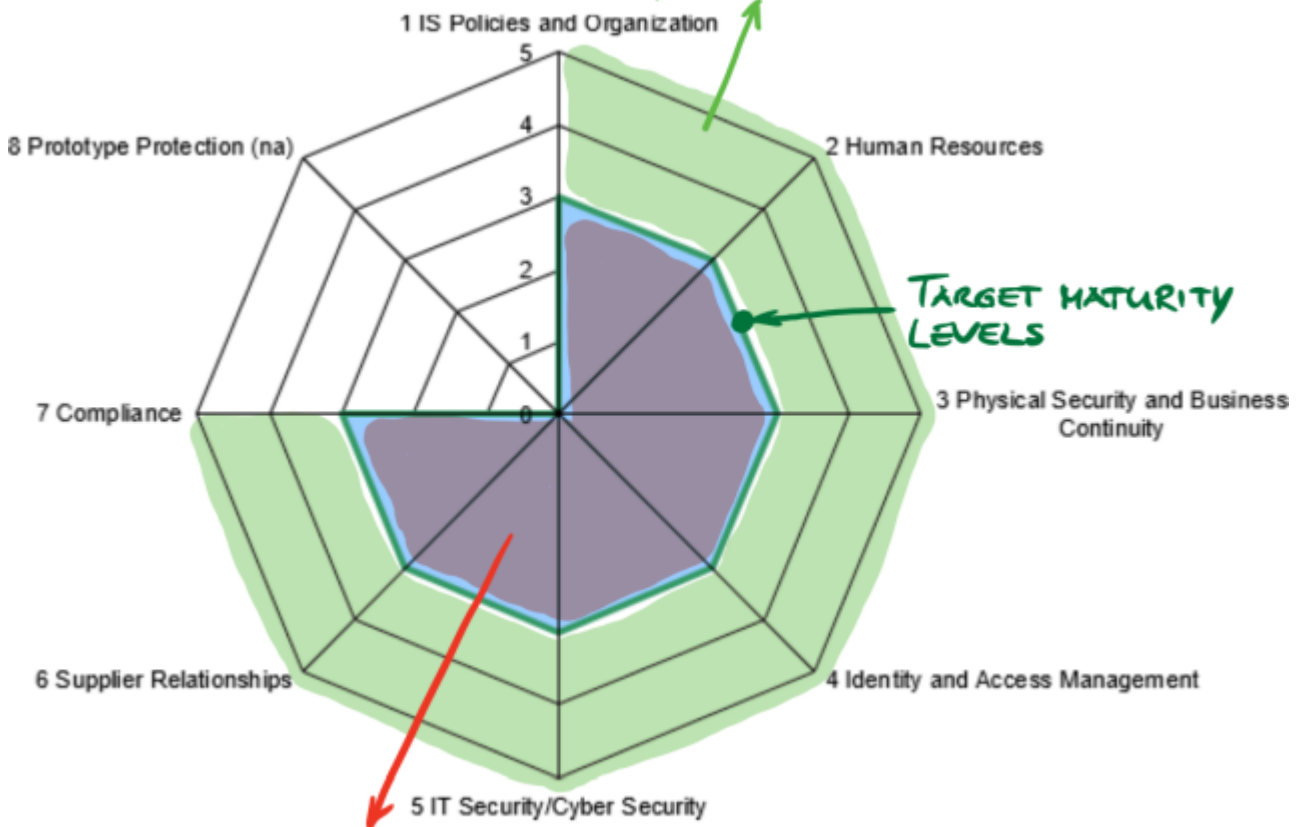
The purpose of the analysis above is to know whether you are ready for a TISAX assessment.

You are definitely ready for a TISAX assessment if your result score (“Result with cutback to target maturity levels”) is (close to) “3.0”. In this case, all values in the “Results” column (H) are green (no orange or red).

If they are not green, you need to address your self-assessment result (please refer to Section 5.2.5, “Address the self-assessment result”).

The figure below shows the ISA spider web diagram on the Excel sheet “Results (ISA5)”. The green line marks the target maturity level per chapter. If your maturity levels are **on or above** that line, you are ready for a TISAX assessment. If they are **below** that line, this may not be sufficient to receive TISAX labels.

You ARE READY FOR A TISAX ASSESSMENT



MATURITY LEVELS MAY NOT BE SUFFICIENT FOR TISAX LABELS!

Figure 29. Screenshot: Target maturity level fulfilment in the ISA spider web diagram (Excel sheet “Results (ISA5)”)

If you “unfold” the ISA spider web to the question level, you get a similar green/red view on the question level:

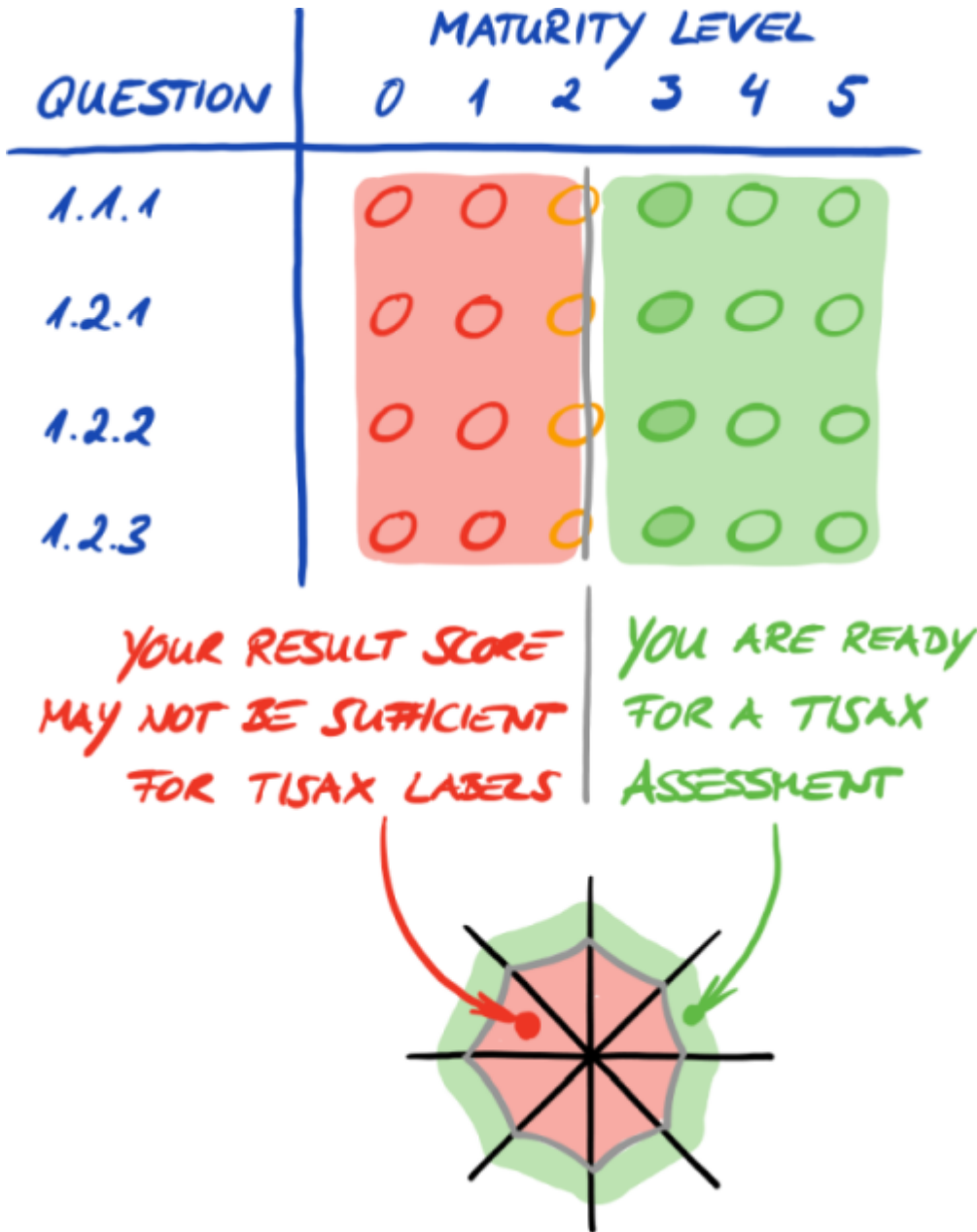


Figure 30. “Unfolding” the ISA spider web diagram

5.2.5. Address the self-assessment result

Your self-assessment result may show that you need to improve your information security management system before you are ready to receive TISAX labels.

For some gaps between your maturity level and the target maturity level, you may already know how to close them. For others, you might need external advice. In this case, you can ask our TISAX audit providers for consulting services. TISAX allows them to consult, but doesn’t require it. Please note that any audit provider doing consulting for you can no longer conduct TISAX assessments for you.



Important note:

Not properly addressing the self-assessment result *before* getting assessed is a major stumbling block for many companies. Please don’t underestimate the effort it may take to shape your information security management system according to the requirements. Many companies need to formally set up a large project to prepare for a TISAX assessment.



Please note:

When you're looking for external help for getting through the TISAX process, you will find that various companies offer consulting and training services. None of these companies are associated with us.

As things currently stand, we:

- don't offer official trainings, either directly or through third parties.
- don't make any statements about the quality of third party services and therefore advise caution.



Please note:

We advise against asking for or ordering items like a "pre-assessment" or a "gap analysis". While we acknowledge the desire to prepare for the assessment in such a way, in almost all cases it makes more sense to start the assessment right away.

For more information on why we advise against pre-assessments, please refer to Section 7.7, "Annex: The reasoning against "pre-assessments" and "gap analyses"".

5.3. Audit provider selection

Only audit providers that we contracted can conduct TISAX assessments^[15] to find out what is required to become a TISAX audit provider. TISAX audit providers are allowed to conduct TISAX assessments for you only if they haven't had any previous consulting assignments with you.

All our TISAX audit providers are obliged to conduct TISAX assessments only for those companies that are registered TISAX participants.



Important note:

Once you have registered a TISAX assessment scope, you *should* start contacting our audit providers. They have a certain lead time regarding their availability. Contacting them *after* you finished your preparations could add an unnecessary delay.



Please note:

Every assessment scope goes through a life cycle. At this stage, your assessment scope must have the status "Approved" or "Registered"

For more information on the status of an assessment scope, please refer to Section 7.5.5, "Assessment scope status "Awaiting your payment"".

5.3.1. Contact information

Once you have registered a TISAX assessment scope, you can contact all TISAX audit providers and request offers. Their contact information is provided in the registration confirmation email you received^[16] (please refer to Section 4.5.8, "Confirmation email").



Please note:

Please request offers from our TISAX audit providers only AFTER you are registered. The audit providers will check for an existing registration. They have to reject requests without registration.

This is also the reason why you receive the audit provider contact information only in the registration confirmation email and not from our public website.

5.3.2. Coverage

While currently many of the audit provider contacts are based in Germany, it is important to understand that all our audit providers are able to generally conduct TISAX assessments worldwide. Most of them even have their own employees in many countries.

On our website, we offer a page where you can select your country and then see which audit provider has local sales staff and/or local auditors (enx.com/en-US/TISAX/xap/).

5.3.3. Requesting offers

In order to allow our TISAX audit providers to precisely calculate the expected assessment efforts, you should always include the “TISAX Scope Excerpt”.



Figure 31. Thumbnail of a scope excerpt (first page)

For more information, please refer to Section 4.5.8, “Confirmation email”.



Please note:

Impartiality is a key characteristic of our TISAX audit providers. They will ensure that no conflict of interest exists. You may want to consider this when contacting them. If your company is somehow related to an audit provider, you can't expect to be assessed by him.

5.3.4. Evaluating offers

You can freely choose among all our TISAX audit providers. They are all bound to the same contract. They all conduct the assessments based on the same criteria and the same auditing methods. In terms of the assessment result, there won't be a difference regardless which audit provider you choose. Your assessment result will be accepted by all TISAX participants.

Besides obvious factors such as price, reputation and likeableness, there are some aspects of an offer you can look for:

- **Availability:** How soon can the assessment process start? This might be an important aspect if getting TISAX-assessed is urgent for you.

- Travel-related costs for on-site appointments: Audit providers with offices in your country might have lower travel-related costs.
- Language: Will you and every other interviewee in your company be able to communicate with the auditor in your native language?
- Which assessments are included?

For more information on assessments, please refer to Section 5.4.3, “TISAX assessment types”.

Usually, the offers include the initial assessment and the corrective action plan assessment. As the efforts for follow-up assessments are difficult to predict, they are typically offered after the other assessments are completed.

Ultimately, it will come down to trust. You will need to form a trust relationship with your audit provider as he will have quite an insight in your company.



Please note:

We advise against asking for or ordering items like a “pre-assessment” or a “gap analysis”. While we acknowledge the desire to prepare for the assessment in such a way, in almost all cases it makes more sense to start the assessment right away.

For more information on why we advise against pre-assessments, please refer to Section 7.7, “Annex: The reasoning against “pre-assessments” and “gap analyses””.



Please note:

While we would certainly like to tell you how much our audit providers will charge for the assessment, we kindly ask for your understanding that it is not possible for us to provide this information. The costs depend on too many factors. On top of that, our audit providers are free regarding their commercial calculations.

However, we can mention some rather rough estimates for how many man-days our audit providers will charge you for. For an average small company with one location, you should expect to pay for three and a half to four man-days for an assessment in assessment level 2 and five to six man-days for an assessment in assessment level 3.



Please note:

Every assessment goes through a life cycle.

For more information on the status of an assessment, please refer to Section 7.6, “Annex: Assessment status”.

Once you’ve chosen one of our TISAX audit providers, you can finally initiate the TISAX assessment process.

5.4. TISAX assessment process

5.4.1. Overview

The TISAX assessment process consists of several types of assessments. In most cases, there will be more than one assessment.

You should view the assessment process as an interlaced sequence of steps where:

- You prepare your information security management system to be in top form.

- The audit provider checks whether your information security management system fulfils a defined set of requirements. He may find gaps.
- You then close the gaps within defined periods.
- The audit provider then checks again whether you closed the gaps.

These alternating steps are done until all gaps are closed.

It is important to understand that *you* initiate each sub-step in the assessment process. The entire assessment process is under your control. And of course it is up to you to stop and exit the assessment process whenever you want.^[17]

The TISAX assessment process has the following macro structure:

- Kick-off meeting
You and the audit provider are planning the details of the assessment process
- Assessment phase 1
The audit provider checks your self-assessment
- Assessment phase 2
The audit provider conducts the assessment(s)

5.4.2. Kick-off meeting

The TISAX assessment process starts with the kick-off meeting. It is the place to plan the details of the assessment process. Usually, the kick-off meeting is done in a conference call. The audit provider will guide you through the meeting.

Among other things, the following topics are on the agenda:

- Who are the meeting participants?
- Who is the assessed company?
- How does the TISAX assessment process work?
- What is the assessment scope and is it the right one?
- Are there no conflicts of interest?
- How does a good self-assessment look like?
- Who is responsible for what?
- How do we communicate?
- When does the assessment take place (and other time planning)?
- Who needs to participate in the assessment(s)?
- Who can you contact when you have complaints?

The period between the end of the kick-off meeting and the delivery of your self-assessment is typically one to three month. But even six month is not unusual. The period depends on the status of your preparation. TISAX does not mandate any deadlines for this period. You can take all the time you need to prepare your self-assessment and to prepare for the assessment.

5.4.3. TISAX assessment types

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

- Initial assessment

- Corrective action plan assessment
- Follow-up assessment ^[18]

The initial assessment will always take place. 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 after the end of the closing meeting of the initial assessment (at which point another initial assessment is required).

All TISAX assessments will be described in the coming sections.



Please note:

Every assessment goes through a life cycle.

For more information on the status of an assessment, please refer to Section 7.6, “Annex: Assessment status”.

5.4.4. TISAX assessment elements

Each TISAX assessment consists of the following elements:

- Formal opening meeting^{[19][20]}
 - It aims to cover all organisational topics.
 - It does not necessarily have to be a physical meeting.
 - Topics can be covered in one go or spread over several occasions.
 - It is a “logical container” for all organisational *pre*-assessment topics.
- Assessment procedure
 - Your audit provider checks all requirements.
 - Assessment methods are selected according to the respective assessment level.
- Formal closing meeting^[21]
 - It concludes a TISAX assessment.
 - The audit provider presents his findings.
 - The audit provider announces the assessment result.
 - It does not necessarily have to be a physical meeting.
 - It is a “logical container” for all organisational *post*-assessment topics.

After the “closing meeting” the audit provider prepares and sends you the draft version of the updated “TISAX assessment report”. You can voice objections if you think the audit provider misunderstood something.^[22] Then the audit provider issues the final “TISAX assessment report”.

All these elements will be described in the next sections.

5.4.5. About conformity

Before we continue outlining the TISAX assessment process, we want to explain you a key concept that is essential for your understanding of the next sections.

The purpose of a TISAX assessment is to determine whether your information security management system fulfils a defined set of requirements. The audit provider checks whether your information security management system “conforms” to the requirements.

Step 1: The checks are made for each applicable requirement individually.

If your approach “conforms” to all requirements, you pass the assessment and receive the TISAX labels that correspond with your assessment objectives.

Everything below full or ideal conformity to the requirements is called a finding. TISAX differentiates four types of findings:

No.	Type	Definition	Reaction	Examples
1.	<i>Major non-conformity</i>	<p>A <i>major non-conformity</i>:</p> <ul style="list-style-type: none"> ▪ creates a significant immediate risk to your information security ▪ or creates doubts regarding the overall effectiveness of your information security management system 	<p>You have to:</p> <ul style="list-style-type: none"> ▪ address <i>major non-conformities</i> immediately with appropriate compensating measures ▪ implement corrective actions without undue delay 	<ul style="list-style-type: none"> ▪ Systematic non-conformities ▪ Implementation deficits that create critical risks to the security of confidential information ▪ Implementation deficits that are not addressed by an appropriate corrective action
2.	<i>Minor non-conformity</i>	<p>A <i>minor non-conformity</i>:</p> <ul style="list-style-type: none"> ▪ does <i>not</i> create a significant immediate risk to your information security ▪ and does <i>not</i> creates doubts regarding the overall effectiveness of your information security management system 	<p>You have to:</p> <ul style="list-style-type: none"> ▪ implement corrective actions without undue delay 	<ul style="list-style-type: none"> ▪ Isolated or sporadic mistakes ▪ Non-compliance or deficits in the implementation of requirements or your policies

No.	Type	Definition	Reaction	Examples
3.	Observation	An observation is a non-compliance with the requirements our your own policies that does not create an immediate risk to your information security but may do so in the future.	You have to: <ul style="list-style-type: none"> ▪ carefully investigate, monitor, and evaluate possible risks ▪ decide how to handle the observation 	n/a
4.	Room for improvement	A deviation that does not belong to aforementioned types and does not create a risk to your information security, yet offers obvious room for improvement.	You can decide whether or how to address this type of finding.	n/a

Table 12. The four types of findings

Step 2: All results of the previous “per-requirement” step are merged into the overall assessment result.

The overall assessment result can be:

a. Conform

The overall assessment result is “conform”. All requirements are fulfilled.

b. Minor non-conform

The overall assessment result is “minor non-conform” if you have at least one “minor non-conformity” for a requirement.

c. Major non-conform

The overall assessment result is “major non-conform” if you have at least one “major non-conformity” for a requirement.

(Without an approved corrective action plan, every non-conformity results in an overall assessment result of “major non-conform”.)

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.

It is important to understand that your overall assessment result will improve during the course of the entire TISAX assessment process.

Please consider this oversimplified example: You may have an overall assessment result of “major non-conform” after the initial assessment. Afterwards you mitigate the corresponding risk. That changes your overall assessment result from “major non-conform” to “minor non-conform”. And once the risk is eliminated, your final overall assessment

result will be “conform”.

All this will be explained below in much more detail. And you can find more about TISAX labels further down in Section 5.4.14, “TISAX labels”.

5.4.6. Your preparation for the TISAX assessment process

The audit provider will prepare the assessment based on your self-assessment. Therefore, please consider that you have to make your self-assessment available to your audit provider ahead of time. The exact delivery deadlines are agreed upon in the kick-off meeting.

A well-prepared audit provider will reduce the time required for the assessment. Besides the self-assessment, he will also request related documentation prior to the assessment. This can be documentation you referenced in the self-assessment and other documentation the audit provider considers relevant.

Based on this information, your audit provider will plan the assessment procedure.

5.4.7. Initial assessment

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



Important note:

The initial assessment marks the start of two important periods:

1. The maximum validity period for TISAX labels is three years.
2. You have up to nine months to resolve non-conformities. If you don't resolve all non-conformities within this period, you won't receive TISAX labels. If you missed this deadline, you can directly continue with a new initial assessment, though.

Both periods start on the day of the closing meeting of the initial assessment.



Please note:

Besides the two periods described above, there are no other time constraints. For example, neither completing the online registration process nor contacting our audit providers or even conducting the kick-off meeting triggers any deadlines. It is up to you to start with the initial assessment.

5.4.7.1. The first formal opening meeting

Like all TISAX assessments, the initial assessment starts with a formal opening meeting. The formal opening meeting is usually done with a conference call or web conference. For small companies, possibly with some experience from other audits, this doesn't take long.

The purpose of this meeting is to:

- check assessment prerequisites
- introduce the assessment project leader and the assessment team
- plan the assessment

5.4.7.2. Assessment procedure

According to the prepared plan, the audit provider conducts the initial assessment. How this will look in detail depends on your assessment objectives. The assessment mainly consists of conference calls, on-site interviews and on-site inspections in varying degrees of depth^[23].

The audit provider presents all his findings during the initial assessment.

5.4.7.3. Closing meeting

In the closing meeting, your audit provider again summarises all his findings.

5.4.7.4. TISAX assessment report

After the closing meeting, the audit provider prepares and sends you the draft version of the “TISAX assessment report”. You can voice objections if you think the audit provider misunderstood something.^[24] Then the audit provider issues the “TISAX assessment report”.

At this stage, the current overall assessment result will either be:

- Conform, or
- Major non-conform
Having unaddressed (minor) non-conformities always results in an overall assessment result of “major non-conform”. Your overall assessment result can only be “minor non-conform” once you defined actions that will implement measures to address the non-conformities.
For more information on how to achieve this, please refer to Section 5.4.9.4, “Temporary TISAX labels”.

If your overall assessment result is “conform” right at the initial assessment, you can skip the rest of the assessment section and proceed to the exchange of your result.

If your overall assessment result is “major non-conform”, your next task is to work out a plan for how to address the findings and how to close any gaps the audit provider found. The plan is officially called the “corrective action plan”.



Please note:

If, before of the assessment starts, you are aware of a situation that will result in a non-conformity, and you won't be able to fix it before the assessment, you could already plan a corrective action (including an implementation date) and present it to the audit provider during the assessment. This, theoretically, could lead to an overall assessment result of “minor non-conform”. However, this would be a *rare* situation.

5.4.8. Corrective action plan preparation

Your “corrective action plan” defines how you plan to address the findings of the initial assessment. Your audit provider will assess the appropriateness of your “corrective action plan” (see next section).

For creating your “corrective action plan”, you should consider the following requirements:

- Finding
 - You need to state which finding the corrective action addresses.
- Root cause
 - You need to identify and state the root cause of the finding.
- Corrective actions
 - For each non-conformity you need to define one or more “corrective actions”, which will implement measures that address the non-conformity.
- Implementation date
 - You need to define an implementation date for each corrective action.

- The implementation period should provide sufficient time to thoroughly implement the measures.
- Compensating measures
 - For all non-conformities that create critical risks, you need to define compensating measures that address the non-conformities until the corrective actions are implemented.
- Implementation period
 - For all corrective actions that take longer than three months to implement, you need to justify the implementation period.
 - For all corrective actions that take longer than six months, you additionally need to provide evidence that shows that a faster implementation is not possible.
 - The implementation period for any corrective action can't be longer than nine months.

Once your corrective action plan is complete, you can request the “corrective action plan assessment”.



Important note:

We recommend starting with the implementation as soon as possible. There is no need to wait for the result of the “corrective action plan assessment”.

The “corrective action plan assessment” usually takes place once you submitted your corrective action plan to your audit provider.



Please note:

TISAX only has requirements with regards to content, not regarding the form of corrective action plans.

Most of our audit providers offer templates for corrective action plans.

5.4.9. Corrective action plan assessment

The purpose of the “corrective action plan assessment” is to verify that your “corrective action plan” (see above) fulfils the TISAX requirements.

You submit your “corrective action plan” to your audit provider. Your audit provider assesses the plan according to the requirements (see below). If your plan fulfils the requirements, your audit provider will issue the updated “TISAX assessment report”.

This assessment usually doesn't take long. In most cases, this will be a conference call or web conference. Sometimes it's even done just by email.

5.4.9.1. Reasons for a corrective action plan assessment

Reasons for a “corrective action plan assessment” are:

- Remaining non-conformities after
 - an initial assessment
 - a follow-up assessment
 - a scope extension assessment
- A “corrective action plan” that already has been assessed, but did not fulfil the requirements
- The influencing factors on which the calculation of the implementation periods of a corrective action plan are based have changed

5.4.9.2. Combination with initial assessment

The “corrective action plan assessment” is not necessarily an independent event. You have the option to already present your “corrective action plan” during the closing meeting of the initial assessment. The audit provider can then directly conduct the “corrective action plan assessment”.

If you combine the “corrective action plan assessment” with the initial assessment, and your “corrective action plan” fulfils the requirements, you can agree with the audit provider that you don’t need an “initial assessment report”. Instead, your audit provider would just prepare the “corrective action plan assessment report”. This report allows you to directly receive temporary TISAX labels.

5.4.9.3. Corrective action plan requirements

The audit provider assesses your “corrective action plan” against the following requirements:

- Measures are appropriate
 - The audit provider will assess the appropriateness of a corrective action based on whether it will resolve the root cause for the non-conformity.
- Critical risks are mitigated with appropriate compensating measures^[25]
- Implementation periods are appropriate
 - Implementation periods start on the day the initial assessment was concluded
- No implementation period is longer than:
 - three months without additional justification
 - six months without additional justification and evidence
 - nine months

5.4.9.4. Temporary TISAX labels

If your overall assessment result is “minor non-conform”, you receive temporary TISAX labels.

The benefit of temporary TISAX labels is that your partner generally accepts them under the condition that you later receive permanent TISAX labels. This may help you if proving the effectiveness of your information security management system to your partner is urgent.

The prerequisite for temporary TISAX labels is a corrective action plan assessment report with the overall assessment result “minor non-conform”.

Temporary TISAX labels are equal to permanent TISAX labels. The only difference is the shorter validity period of temporary TISAX labels.

Temporary TISAX labels can be valid for up to nine months after the closing meeting of the initial assessment. The validity period of the temporary TISAX labels is determined by the longest implementation period of the corrective actions.

Examples:

- You have only one non-conformity. You have to do a policy review. The associated implementation period is *two* month.
Then your temporary TISAX labels are valid for *two* month.
- You have the non-conformity of the aforementioned policy review. On top, you have a non-conformity where you have to build a new outer wall as a corrective action. Due to the time it takes to obtain the required approvals from the municipality, the associated implementation period is *eight* month.

Then your temporary TISAX labels are valid for *eight* month.

For more information on the requirements for implementation periods, please refer to Section 5.4.9.3, “Corrective action plan requirements”



Please note:

The “corrective action plan assessment” is optional.

You can proceed straight to the follow-up assessment if you:

- don’t need temporary TISAX labels and
- are confident to implement any corrective actions without getting your plan approved by your audit provider

Once you’ve completed all corrective actions, you should request the “follow-up assessment”.

5.4.10. Follow-up assessment

The purpose of the “follow-up assessment” is to assess whether all previously identified non-conformities are resolved. Usually you request the follow-up assessment once you are sure that all non-conformities are resolved.

But you can have as many follow-up assessments as you need. If during a follow-up assessment your audit provider still attests existing or even new non-conformities, you simply update your corrective action plan and start this part of the assessment process again.

This assessment can be a physical meeting as well as a conference call or web conference.

5.4.10.1. Timing

Your audit provider can conduct the follow-up assessment(s) within up to nine months after the conclusion of the initial assessment^[26].

5.4.10.2. Prerequisites

If you don’t need temporary TISAX labels, you can directly request a follow-up assessment. You don’t need to have a “corrective action plan assessment” prior to a follow-up assessment.

5.4.10.3. Expiration of temporary TISAX labels

In case you need temporary TISAX labels, you may want to ensure there is no gap to receiving the permanent TISAX labels. We therefore recommend requesting your follow-up assessment well ahead of the latest possible date^[27]. The reason is that you want to have enough buffer time to address any minor findings identified during a follow-up assessment.

5.4.11. TISAX assessment process diagram

The previous sections are now summarised in the following process diagram:

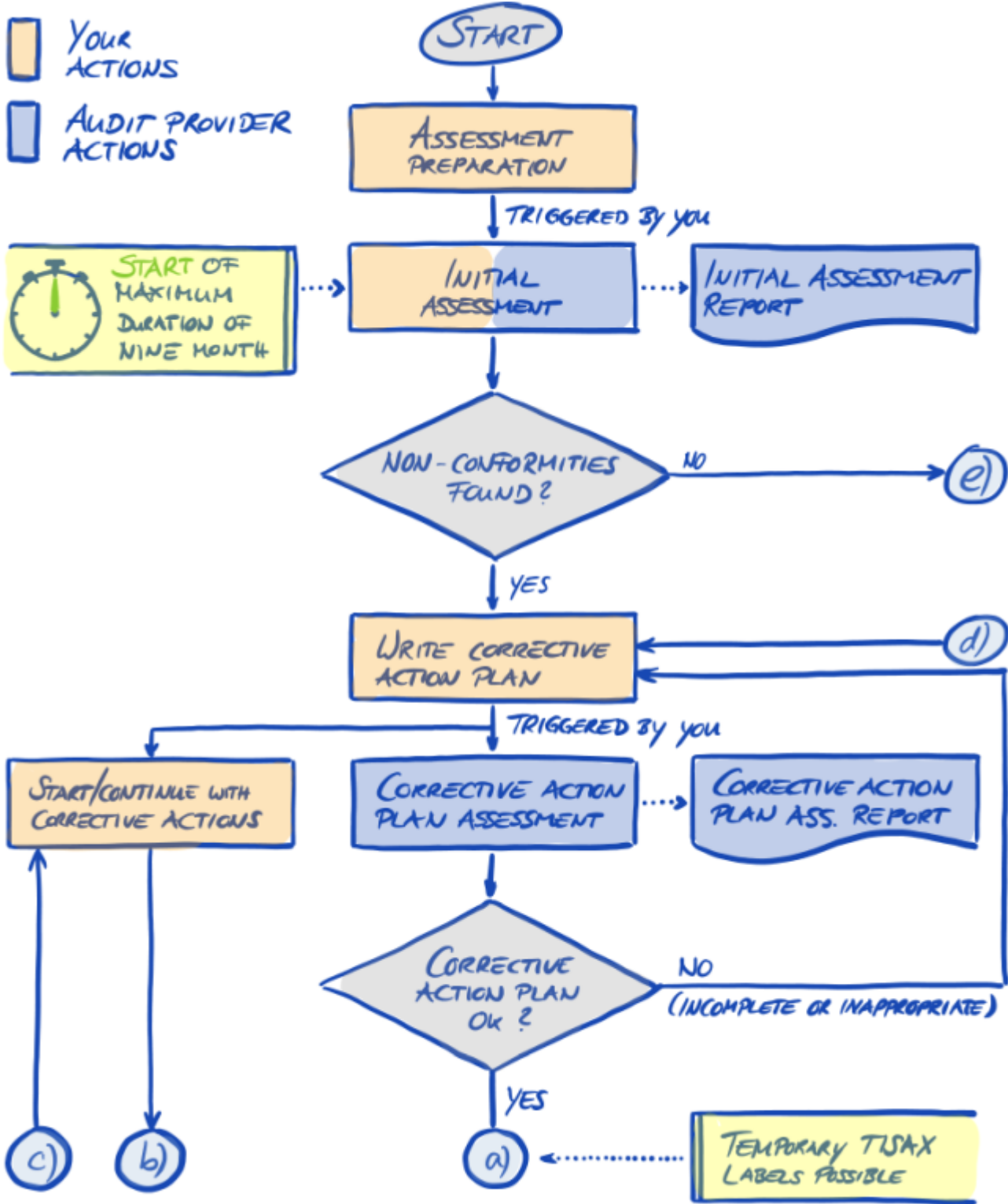


Figure 32. TISAX assessment process diagram (part 1/2)

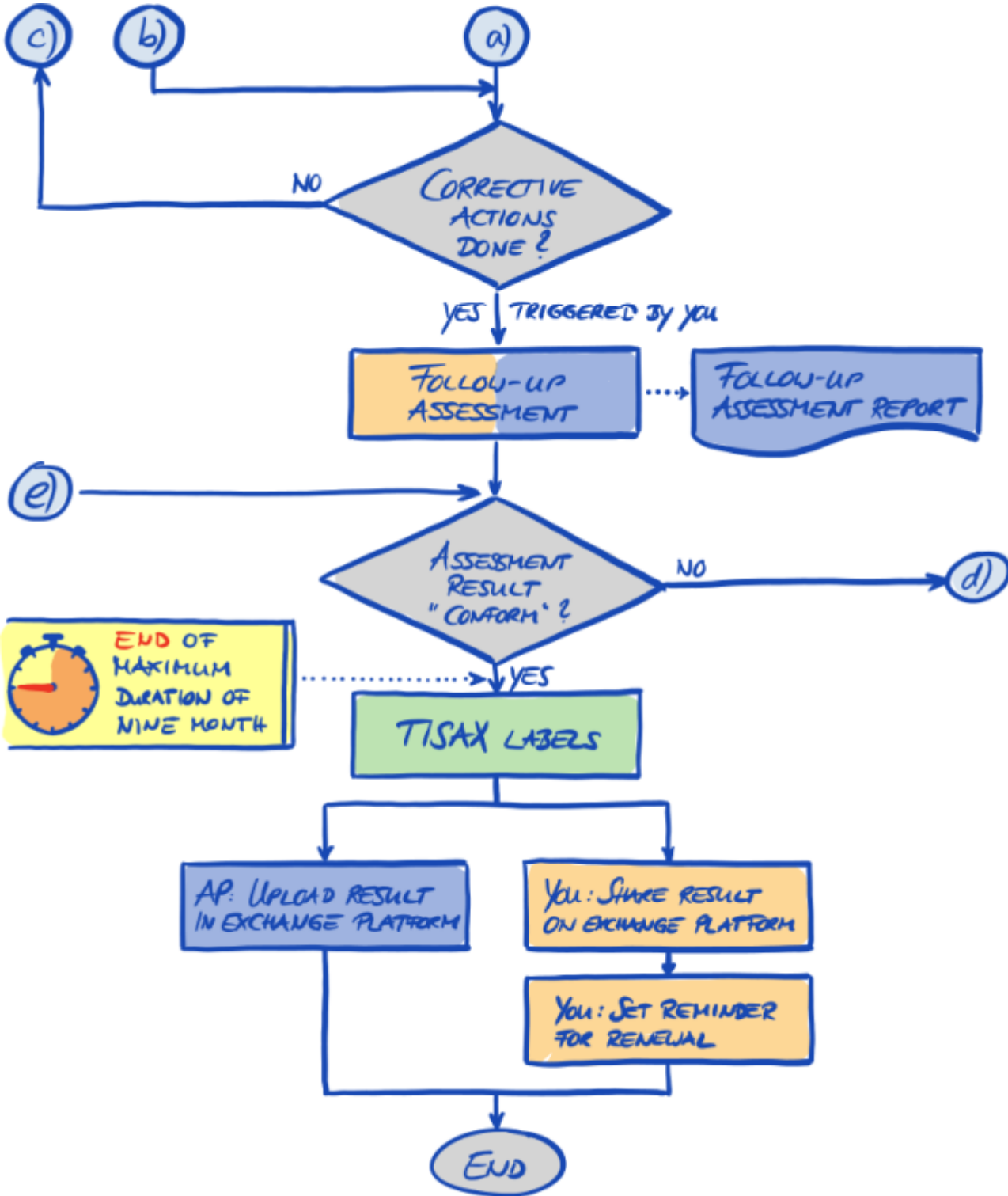


Figure 33. TISAX assessment process diagram (part 2/2)

5.4.12. Assessment ID

Each TISAX assessment of an assessment scope is identified by an “Assessment ID”. This ID refers to your assessment result and the corresponding TISAX assessment report.

This is what the Assessment ID looks like:

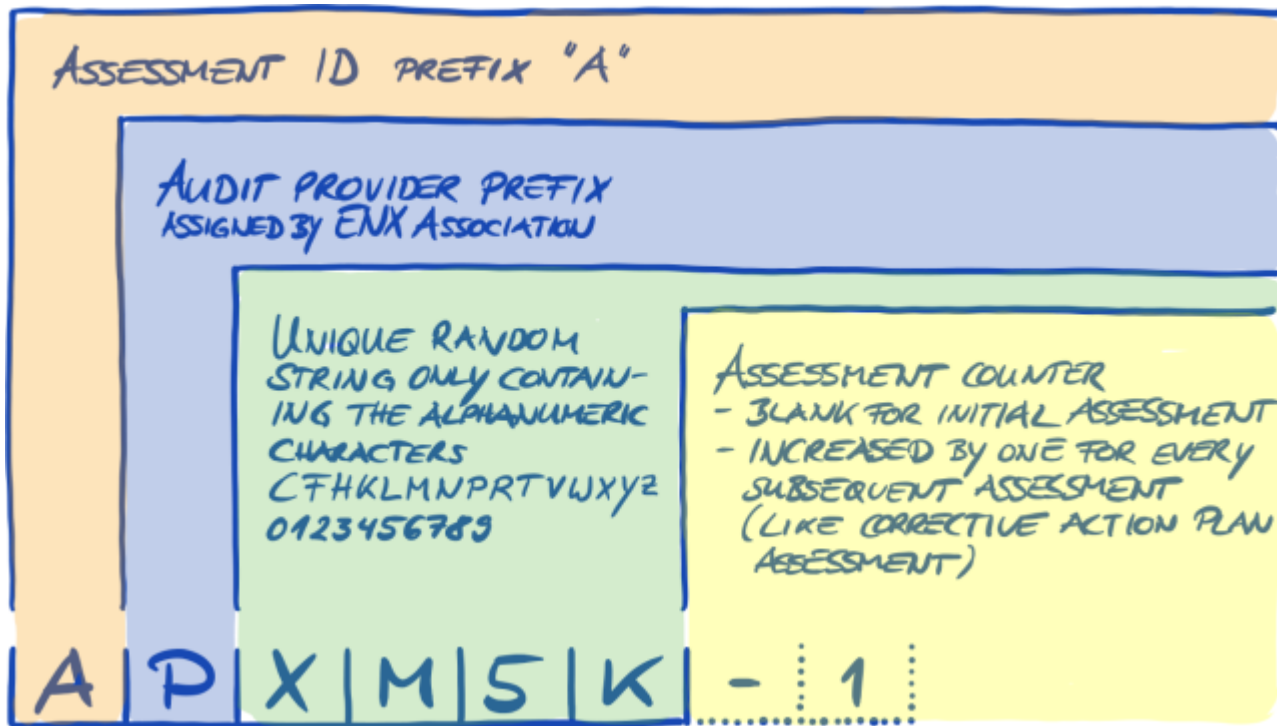


Figure 34. Format of the Assessment ID

The Assessment ID is typically used when your audit provider communicates with you.

5.4.13. TISAX assessment report

The "TISAX assessment report":

- is (updated and) issued after each TISAX assessment.
- documents your audit provider's findings.
- contains the overall assessment result (conform, minor non-conform, major non-conform).
- contains all other information related to your TISAX assessment (such as assessment objective, scope, involved people and locations).

The "TISAX assessment report" can be of the following types (depending on the type of assessment):

- *Initial* assessment report
- *Corrective action plan* assessment report
- *Follow-up* assessment report ^[28]

The "TISAX assessment report" always has the same structure^[29]. Your audit provider simply extends it after each type of assessment. This means you only need to deal with the last version of the TISAX assessment report as it always contains the content of its older version(s).

The first sections of the "TISAX assessment report" is what you ultimately share with your partner.

It is one of the key features of TISAX that it is totally up to you to decide which parts of the TISAX assessment report you want to share with your partner or any other participant. The structure of the TISAX assessment report is designed to enable this kind of selective sharing. Each section expands the level of detail.

Here is what the structure of the "TISAX assessment report" looks like:

- A. Assessment Related Information
Company name, assessment scope, Scope ID, Assessment ID, assessment level, assessment objective(s), assessment date(s), audit provider
This section does not contain any assessment result.
- B. Summarized Results
Management summary of the assessment result (conform, minor non-conform, major non-conform), number of findings, abstract categorisation of resulting risks
- C. Assessment result summary
Summary of the assessment result per chapter (for example “9 Access Control”) and per criteria catalogue (for example “Information Security”)
- D. Maturity Levels of VDA ISA (Result Tab)
Maturity level for each requirement
- E. Detailed Assessment Results
Detailed description of all findings, corresponding risk assessment results, required measures, implementation period

In the “exchange” step (detailed below) you decide up to which level your partner will have access to the content of your TISAX assessment report.

5.4.14. TISAX labels

We briefly touched on this topic in the registration preparation section. As explained, what once was an assessment objective now became a TISAX label.

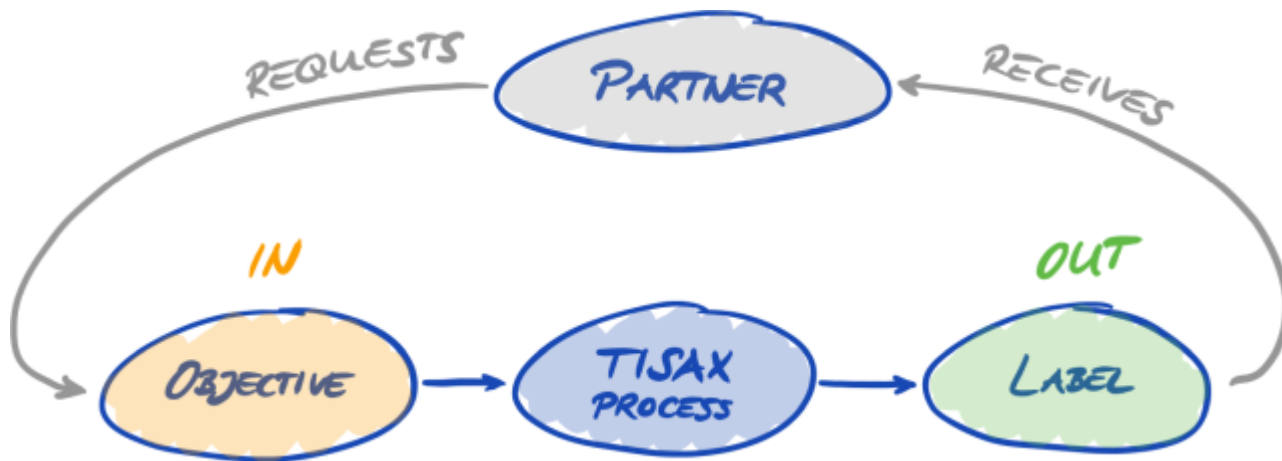


Figure 35. Assessment objectives and TISAX labels

The TISAX labels:

- are the outcome of the TISAX assessment process.
- summarise your assessment result.
- are the statement that your information security management system fulfils a defined set of requirements.

The use of TISAX labels makes the TISAX-related communication with your partner and your TISAX audit provider easier because they refer to a defined output of the TISAX assessment process.

5.4.14.1. TISAX label hierarchy

The mapping between any assessment objective and the corresponding TISAX labels is pretty straightforward. But there is another important aspect: Some TISAX labels are hierarchically linked. This means that if you receive a certain TISAX label, you automatically receive all TISAX labels “below” that particular label.

Example (with abbreviated label names): If your assessment objective was “Info very high”, you receive the corresponding TISAX label “Info very high”. But because the assessment objective “Info very high” is a superset of “Info high”, you automatically receive the TISAX label “Info high”, too.

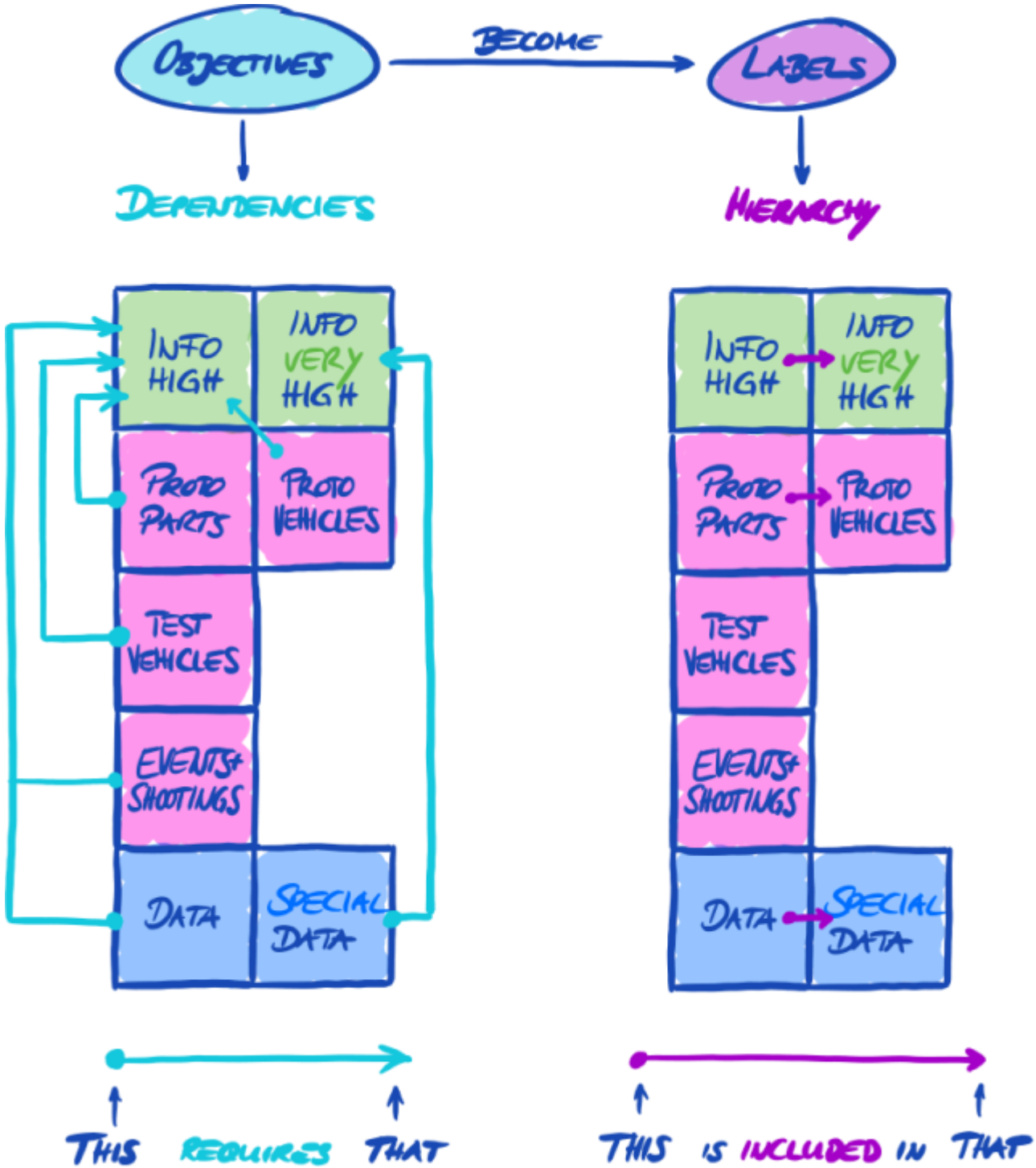


Figure 36. TISAX assessment objectives and TISAX labels (dependencies and hierarchy)

This might not seem important for every participant. But imagine one partner requests you to show the TISAX label “Info very high” and another one requests the TISAX label “Info high”. Then having both TISAX labels makes it easier for everyone because no one needs to understand that “Info high” is a subset of “Info very high”. This may be

particularly true for partners where having certain TISAX labels is part of rather stringent purchasing process. You surely won't want to explain that "Info very high" is "better" than "Info high". You just show all your TISAX labels and the person doing the evaluation can simply check off the requirement "must have TISAX label 'Info high'".

5.4.14.2. Validity period of TISAX labels

TISAX labels are generally valid for three years. The validity period starts at the end of the assessment process (even before the TISAX assessment report is issued).

Their validity period might be shorter if something significant regarding the TISAX assessment scope changes.

Examples: relocation of your company, new locations. (For instructions on what to do in such cases, please refer to Section 7.9.3.2, "How to request the change of a location" and Section 7.9.3.4, "How to add an additional location".)



Please note:

You can view your TISAX labels in the ENX portal only. They are not recorded in the TISAX assessment report.

5.4.14.3. Renewal of TISAX labels

To keep your TISAX labels long-term, you need to renew^[30] them every three years.

For this you basically need to run through the TISAX process again (register an assessment scope, get TISAX-assessed again, share your assessment result). The registration is somewhat easier as you don't need to re-create your company as a TISAX participant. And you can of course re-use all your contacts and locations that are already stored in the TISAX database.



Important note:

Please register a NEW scope BEFORE approaching your audit provider. Your audit provider can start a new assessment process only if you can provide a new Scope ID.

In most cases, registering a new scope is easy. You just need to assign a new scope name, add contacts, select the assessment objective(s) and add locations. You can re-use contacts and locations that are already in the system from any previously registered scope.



Important note:

Please reuse the existing location records that you created and used during the registration of your previous scope. Don't create a new location record with the same address.

The reason for this: Some TISAX participants process the assessment results of their partners automatically. They synchronise their own system with the ENX portal. Even tiny differences may block the successful synchronisation. Besides that, you don't clutter your participant data with unnecessary duplicates.



Important note:

If always having valid TISAX labels during the relationship with your partner is a requirement, we strongly advise that you put a reminder in your calendar to start the necessary renewal process.

We recommend starting the renewal at least one year before your TISAX labels expire.

Now that you received your TISAX labels, you can proceed to the last step and share them with your partner.

6. Exchange (Step 3)

The estimated reading time for the exchange section is 7 minutes.

You have gone through the TISAX process so far, but your partner still has not seen any “proof” that your information security management system is capable of protecting his confidential data. This section now describes how to share your assessment result with your partner and present the requested proof.

6.1. Premise

It is one of TISAX’ key features that your assessment result is fully under your control. Without your explicit permission, all information related to your assessment is not shared with anyone.


6.2. The exchange platform

The ENX portal (<https://enx.com/en-US/TISAX/>) provides the exchange platform.

Your audit provider will upload the first two sections (A and B) of your TISAX assessment report. At this stage, the information is not available to anyone except you.

You can use the account created during the registration to access the portal and use the exchange platform.

You can access the portal at this address:

 enx.com/en-US/SignIn

6.3. General prerequisites

You can share your assessment result with your partner only if these two prerequisites are fulfilled:

1. Your audit provider has submitted the assessment result to the exchange platform.
The assessment result will be available on the exchange platform usually 5-10 business days after the TISAX assessment report is issued.
2. We have received your payment for the fee (if applicable).

The status of your assessment scope is “Active” when both prerequisites are fulfilled.



Please note:

Every assessment scope goes through a life cycle. At this stage, your assessment scope must have the status “Active”.

For more information on the status of an assessment scope, please refer to Section 7.5.5, “Assessment scope status “Awaiting your payment””.

To verify whether your assessment result is ready for sharing (assessment scope status = Active), follow these steps:

1. Log in to the ENX portal (<https://enx.com/en-US/TISAX/>).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “SCOPES AND ASSESSMENTS”.
4. Go to the table and find the table row with your assessment scope.

5. Verify that your assessment scope has the assessment scope status “Active” (column “Scope Status”).

6.4. Permanence of exchanged results



Important note:

You can't revoke any publication or sharing permissions.

The reason is that we want that all passive participants can rely on continual access to every assessment result they received. Otherwise they would have to manage and archive the assessment results on their own.

The permission remains valid for the complete validity period of your TISAX assessment.

If you created a publication or sharing permission by mistake, please contact us immediately.

6.5. Sharing levels

The sharing levels map 1:1 to the main sections A-E of the TISAX assessment report.

	Main sections of the TISAX assessment report	Sharing levels on the exchange platform
1	A. Assessment Related Information	
2	B. Summarized Results	
3	C. Assessment result summary	
4	D. Maturity Levels of VDA ISA (Result Tab)	
5	E. Detailed Assessment Results	

Table 13. Main sections of the TISAX assessment report and the sharing levels on the exchange platform

The higher the sharing level, the more detail about your TISAX assessment will be accessible for the respective participant(s).

For more details on the content of each section of the TISAX assessment report, please refer to Section 5.4.7.4, “TISAX assessment report”.

6.6. Publish your assessment result on the exchange platform

You can share your assessment result with all other TISAX participants by publishing it on the exchange platform. Doing so allows all other TISAX participants to access your assessment result up to the granted shared level.

You can only publish your assessment result if the overall assessment result is “conform”.

The sharing levels for publishing your assessment result on the exchange platform are limited to these options:

- Do not publish (Default)
- A. Assessment Related Information
- A + Labels
- A + Labels + B. Summarized Results


We recommend the sharing level “A + Labels” for this general type of publication.

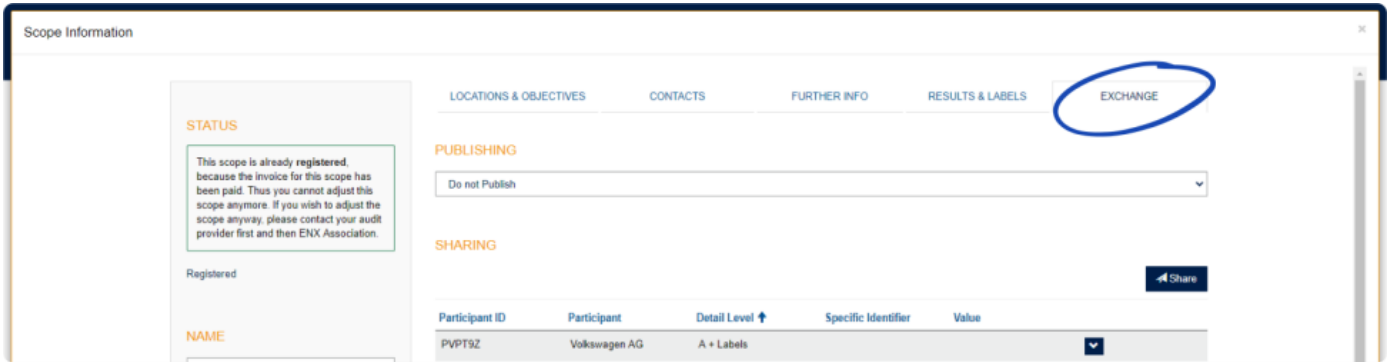


Important note:

You can publish your assessment result only if the prerequisites described in Section 6.3, “General prerequisites” are fulfilled.

To publish your assessment result on the exchange platform, follow these steps:

1. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “SCOPES AND ASSESSMENTS”.
4. Go to the table and find the table row with your assessment scope.
5. Verify that your assessment scope has the assessment scope status “Active” (column “Scope Status”).
6. Go to the end of the table row of your assessment scope and click the button with the down arrow .
7. Select “Scope Information”.
8. In the new window (“Scope Information”), select the tab “EXCHANGE”.



9. Go to the section “PUBLISHING”, open the dropdown menu, and select the desired sharing level (see recommendation above).



Please note:

The assessment results are published on the exchange platform only. They can be accessed by other TISAX participants only. There is no public listing of all TISAX participants. Only the raw number of TISAX participants may be mentioned on the public TISAX website.

6.7. Share your assessment result with a particular participant

Besides the aforementioned option to publish your TISAX assessment result on the exchange platform, you can share it selectively with particular TISAX participants with a higher sharing level.

In contrast to the aforementioned publication, you can share your assessment result even if the overall assessment result is (major/minor) non-conform.

Sharing assessment results is an integral part of TISAX. You only had your information security management system assessed once, but now you can share your assessment result with as many partners as you like.

The options for sharing your assessment result on the exchange platform are:

1. A: Assessment Related Information

2. A + Labels
3. A + Labels + B: Assessment Summary
4. A + Labels + B + C: Summarized Results
5. A + Labels + B + C + D: Detailed Assessment Results
6. A + Labels + B + C + D + E: Maturity Levels according to ISA

We recommend the sharing level “A + Labels” for sharing. This is sufficient for the majority of partners. You can always select a higher sharing level later.



Please note:

Some TISAX participants process the assessment results of their partners automatically. They synchronise their own system with the ENX portal. Only assessment results shared specifically with this participant are synchronised. A publication alone, as described in Section 6.6, “Publish your assessment result on the exchange platform”, is not recognised.

Among the OEMs using TISAX, BMW is an example of this. If you are a partner of BMW, please ensure to share (not just publish) your assessment result with BMW.

6.7.1. Prerequisites

These are the prerequisites for sharing your assessment result with your partner (or any other TISAX participant):

- You can share your TISAX assessment result only with other TISAX participants.
- Your partner needs to be a TISAX participant.
- You need the Participant ID of your partner.^[31]
- You need to pay the fee (if applicable).




Important note:

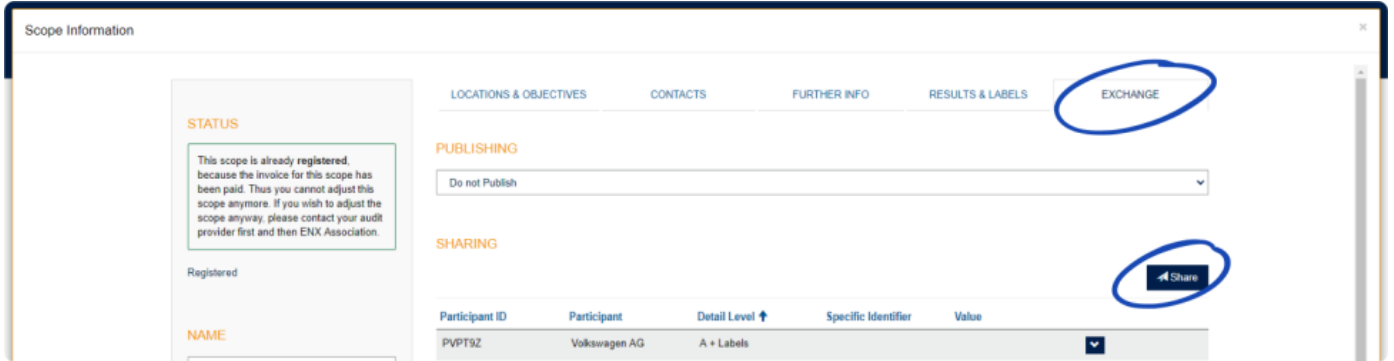
You can share your assessment result only if the general prerequisites described in Section 6.3, “General prerequisites” are fulfilled.

6.7.2. How to create a sharing permission

To share your assessment result with another TISAX participant, follow these steps:

1. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “SCOPES AND ASSESSMENTS”.
4. Go to the table find the table row with your assessment scope.
5. Verify that your assessment scope has the assessment scope status “Active” (column “Scope Status”).
6. Go to the end of the table row of your assessment scope and click the button with the down arrow .
7. Select “Scope Information”.

8. In the new window (“Scope Information”), select the tab “EXCHANGE”.



9. Go to the section “SHARING” and click the button “Share”.

10. In the new window (“SHARE THIS SCOPE”), enter your partner’s Participant ID (or select him from the participant list in the neighbouring search box).

11. Select the desired sharing level.

12. Click the button “Next”.

13. Read and understand the instructions regarding the permanence of the sharing permission.

14. Mark the two “confirm” check boxes.

15. Click the button “Submit”.

Everything else is done by the exchange platform. For sharing level A and B, the information is available on the exchange platform. Your partner can now log into the ENX portal and see your shared assessment result^[32].

For higher sharing levels (C-E), the exchange platform notifies your audit provider. Then your audit provider sends the information (matching the selected sharing level) to the main participant contact of your partner.

6.8. Sharing your assessment result outside TISAX

The rule^[33] is that you can use the TISAX exchange platform only to let other TISAX participants know about your assessment result.

6.8.1. The reasons for the strict governing of the exchange mechanism

TISAX provides a standardised exchange mechanism for assessment results. This provides an added value in comparison to the exchange of the results of other certifications (e.g. ISO), where this happens in various ways and does not always contain all the information required for the complete picture.

OEMs in particular appreciate this standardisation. But other companies also benefit from clearly defined procedures.

6.8.2. A guide to writing about TISAX in public

While you can’t publicly write about the assessment result, you can mention your TISAX efforts. On the ENX portal, we provide advice on how to approach public statements. We also provide TISAX logos you can use.

After logging in into the ENX portal, you can access the information here:

enx.com/en-US/myenxportal/marketing/

Direct ZIP archive download (document and logos):

enx.com/myenxportal/marketing/tisax-trademark-and-logos-guidelines

In case you are wondering whether there’s a certificate you could hang on your wall:

Due to the standardised exchange process mentioned above we don’t provide such a certificate.

6.8.3. Sharing with a partner who is not yet a TISAX participant

If you want to share your TISAX assessment result with a particular partner who is a) not yet a TISAX participant and has b) not yet received TISAX labels (by going through the assessment process), you can follow these steps:

1. Instruct your partner to register as a TISAX participant.

He just has to register as a TISAX participant. He doesn't need to continue to register an assessment scope.

2. Instruct your partner to contact us.


Usually, we process a new registration only if the company also registers an assessment scope. On request by your partner, we process his registration. Thus, he will become a TISAX participant. He can now receive your TISAX assessment result through the regular exchange process.

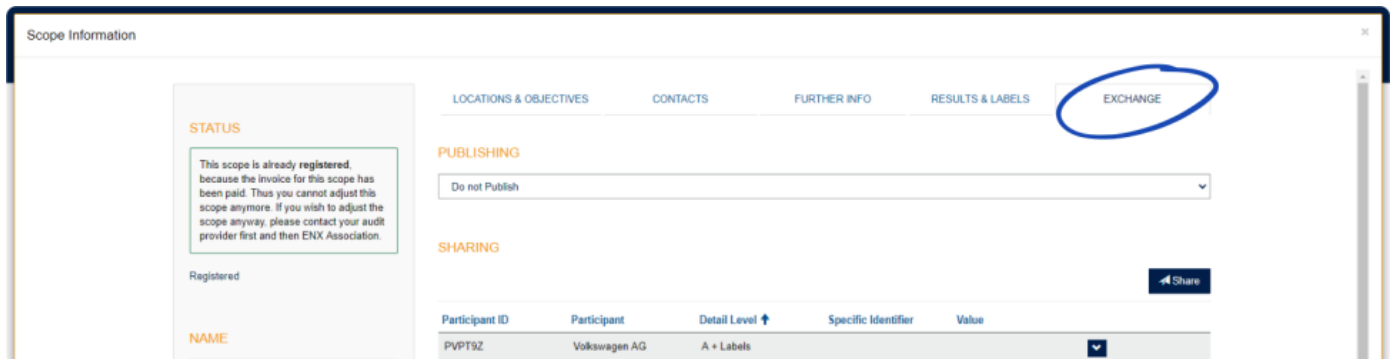
The purpose of this approach is to ensure that your partner agrees to adhere to the "TISAX Participation General Terms and Conditions" that govern the exchange of TISAX assessment results.


Only the registration of an assessment scope incurs costs. Because registering as a TISAX participant is free, your partner can receive your assessment result for free. However, without an own assessment result, your partner can receive only up to five assessment results and can't see any of the publications.

6.8.4. Sharing with employees of your partner who have no direct access to the ENX portal

Only those employees of your partner that have an account for our ENX portal can directly see your result. If you need to prove your TISAX labels to an employee of your partner without portal access, you can use a special PDF document for this. To obtain the document, please follow these steps:

1. Share your assessment result with your partner as described in Section 6.7, "Share your assessment result with a particular participant".
2. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).
3. Go to the main navigation bar and select "MY TISAX".
4. From the dropdown menu, select "SCOPES AND ASSESSMENTS".
5. Go to the table and find the table row with your assessment scope.
6. Verify that your assessment scope has the assessment scope status "Active" (column "Scope Status").
7. Go to the end of the table row of your assessment scope and click the button with the down arrow .
8. Select "Scope Information".
9. In the new window ("Scope Information"), select the tab "EXCHANGE".



10. Go to the section "SHARING" and find the table row with the sharing permission (as created in step 1).
11. Go to the end of the table row of the sharing permission and click the button with the down arrow .
12. Select "Edit"
13. In the new window ("SHARE THIS SCOPE"), scroll to the bottom and select "Request Shared Information as PDF".

14. Wait a moment until the document is generated.
15. Download the document (“Copy of information shared with ACME.pdf (66.84 KB)”)

7. Annexes

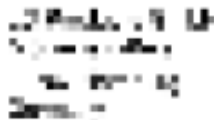
7.1. Annex: Example invoice

This is an example of the invoice we send.

For more information, please refer to Section 4.3.4, “Fee”.



ENX Association • Bockenheimer Landstr. 97-99 • D 60325 Frankfurt am Main



INVOICE / RECHNUNG

Invoice Number / Rechnungsnummer
30.06.2020
 Invoice Date / Rechnungsdatum
Net 30 Days
 Payment Conditions / Zahlungsbedingungen
 Your Purchase Order Number / Ihre Bestellnummer
 Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
 Period of Service / Leistungszeitraum
Rodryk Olejnik
 Contact in your organization / Ansprechpartner bei Ihnen
rodryk.olejnik@loproducts.de
 Contact in your organization / Ansprechpartner bei Ihnen

Pos.	Prod.ID/ Art.-Nr.	Qty/ Anz.	Unit/ Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9011	1	Loc	Assessment Based Charges for TISAX Scope	405,00 €	405,00 €
Net Amount / Netto						405,00 €
VAT / MwSt (19,00%)						76,95 €
Gross Amount / Brutto						481,95 €

Please transfer the gross amount without deductions and with reference to the invoice number to our bank account. Bank service charges must be paid by the remitter.

ENX Association

Address
 ENX Association
 Bockenheimer Landstr. 97-99
 60325 Frankfurt am Main
 Germany

Contact
 Phone +49 69 9866927-0
 Fax +49 69 9866927-99
 Email info@enx.com
 Contact ar@enx.com

Bank Account
 IBAN: DE36 5005 0201 0000 3067 89
 Swift/BIC: HELADEF1322
 Bank: Frankfurter Sparkasse
 Post-Addr.: 60325 Frankfurt/Main, Germany

Registration of the Association
 Registered at Boulogne-Billancourt, France
 under Registration-No. W923004195
 VAT-ID: DE313277692
 President: Philippe Ludet

7.2. Annex: Example confirmation email

We send the confirmation email once you completed all the mandatory steps during the online registration process.

For more information when we send this confirmation email, please refer to Section 4.5.8, “Confirmation email”.

Subject: [TISAX] Scope S3ZY5V Approved

Dear John Doe

Thank you for the TISAX assessment scope registration. I have carried out your scope registration and approved your scope. Attached you can find the TISAX scope excerpt including all scope information and the current TISAX audit provider list.

What's next?

With the attached TISAX scope excerpt you can now request quotes from all TISAX audit providers for your scope.

Assistance needed?

For further questions regarding TISAX, please read the TISAX FAQs or the TISAX Participant Handbook. If you need further assistance regarding TISAX, please do not hesitate to contact the TISAX hotline via email (tisax@enx.com) or via phone (+49 69 986692-777).

Kind regards,

Your TISAX Team

7.3. Annex: Example TISAX Scope Excerpt

You receive the “TISAX Scope Excerpt” attached to the confirmation email.

For more information, please refer to Section 4.5.8, “Confirmation email”.

TISAX Scope Excerpt S3ZY5V

Participant: ACME Lt. (PXLNC58)



Scope: ACME Ltd.		S3ZY5V	
Standard Scope 1.0			
The Scope comprises all processes and involved resources at the sites defined below that are subject to security requirements from partners in the automotive industry. Involved processes and resources include collection of information, storage of information and processing of information.			
Assessment Objectives		AL	Locations
Information with Very High Protection Needs		3	1
Maturity of ISMS	Certified on	Certified in	
Complexity of ISMS	Justification (only if simple ISMS)		
Use of Consulting Firm for ISMS	Name of Consulting Firm		
Earliest Kickoff-Meeting	Labels needed until	External Requirement	

Location: Frankfurt		
Company Name and Address	Location-ID	DUNS
ACME Ltd. Bockenheimer Landstr. 97-99 60325 Frankfurt Germany	L5WDZR	812533185
	Type	
	Building(s) rented by company	
	Passive Site Protection	Employees
	Yes	Overall: 11-100
	Industry	IT: 1-10
	Telecommunication Services;	IT-Security: Part Time
		Location Security: 0

7.4. Annex: Participant status

7.4.1. Overview: Participant status

The “participant status” defines where you (as a company) are in the TISAX process.

Your “participant status” can be:

1. Incomplete
2. Awaiting approval
3. Preliminary
4. Registered
5. Expired

The tables in each status’ section below describe:

- your situation
(what’s true right now when you are at this status)
- your next action
(what you need to do to progress to the next status; if applicable)
- our next action
(what we need to do to elevate your status; if applicable)
- the next status
(if applicable)

The following illustration shows the actions that lead to progress from one status to the next:

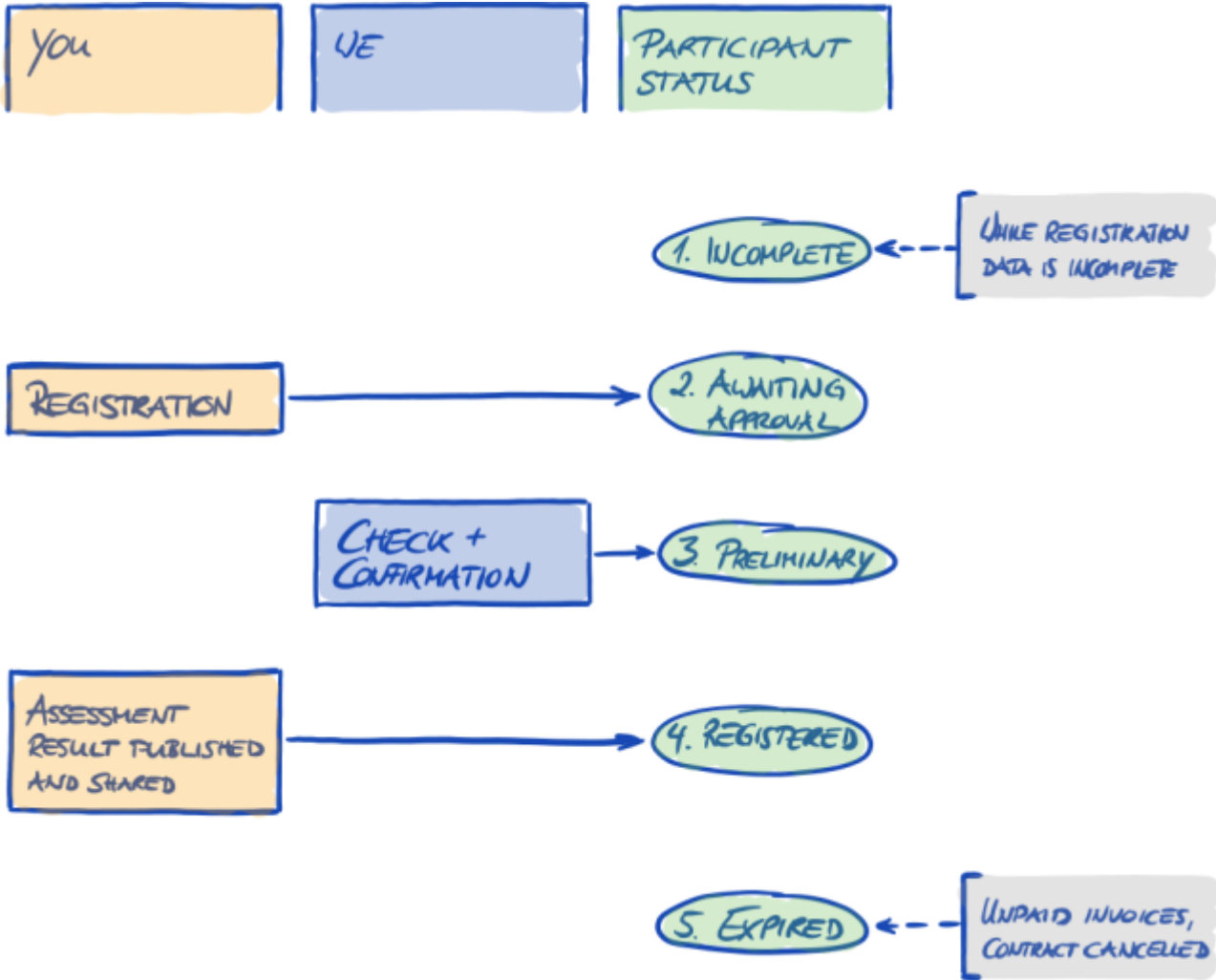



Figure 37. Participant status overview

7.4.2. Participant status “Incomplete”

Status	Situation	Your next action	Our next action	Next status
Incomplete	<p>You have not completed the TISAX registration.</p> <p>Either you have not accepted the general terms and conditions.</p> <p>Or you have not specified the main participant location.</p> <p>Or you have not assigned a main participant contact.</p> <p>Or other information we require is missing.</p>	<p>Continue at  enx.com/en-US/SignIn</p>	<p>We will send you a reminder by email (usually within a few days).</p>	Awaiting approval

7.4.3. Participant status “Awaiting approval”

Status	Situation	Your next action	Our next action	Next status
Awaiting approval	Your TISAX registration is complete. You may or may not have registered an assessment scope yet.	Wait for our next action.	We will check and typically approve your application. However, you usually trigger our checking by also registering an assessment scope. We will assign a Participant ID and the Scope ID(s). We will send you a confirmation email. The attached "TISAX Scope Excerpt" (PDF) summarises the information we have in our database.	Preliminary

7.4.4. Participant status "Preliminary"

Status	Situation	Your next action	Our next action	Next status
Preliminary	You have successfully completed the TISAX registration process.	Pay the fee (if applicable). Go through the TISAX assessment process. Publish and share your assessment result.	None	Registered

7.4.5. Participant status "Registered"

Status	Situation	Your next action	Our next action	Next status
Registered	<p>You have successfully completed the TISAX assessment process and received TISAX labels.</p> <p>You have published and shared your assessment result.</p> <p>You receive TISAX labels only when you successfully passed the TISAX assessment process.</p> <p>In the ENX portal, this is reflected by having an assessment scope with the assessment scope status “Active”.</p>	None	None	(Expired)



Please note:

If you want to access the assessment results of your partner(s):

The conceptual prerequisite for being able to receive assessment results of other participants is either:

- You share your own assessment result (this “proves” that you are a serious TISAX participant and a member of the automotive community).
- We acknowledge you based on your reputation in the automotive industry (like OEMs, tier 1 suppliers).
- You prove that you have a legitimate interest in receiving assessment results from other participants. We have to verify this in an elaborate process that can incur a substantial fee. For further details, please contact us.

7.4.6. Participant status “Expired”

Status	Situation	Your next action	Our next action	Next status
Expired	<p>You have not paid the fee.</p> <p>Or you or we have cancelled our mutual contract (the GTCs).</p>	None	None	n/a

7.5. Annex: Assessment scope status

7.5.1. Overview: Assessment scope status

The “assessment scope status” defines where your assessment scope is regarding its life cycle.

Please be aware that the “assessment scope status” is different from the “assessment status”. For more information on the “assessment status”, please refer to Section 7.6, “Annex: Assessment status”.

Your “assessment scope status” can be:

1. Incomplete
2. Awaiting your order
3. Awaiting ENX approval
4. Awaiting your payment
5. Registered
6. Active
7. Expired

The tables in each status’ section below describe:

- your situation
(what’s true right now when you are at this status)
- your next action
(what you need to do to progress to the next status; if applicable)
- our next action
(what we need to do to elevate your status; if applicable)
- the next status
(if applicable)

The following illustration shows the actions that lead to progress from one status to the next:

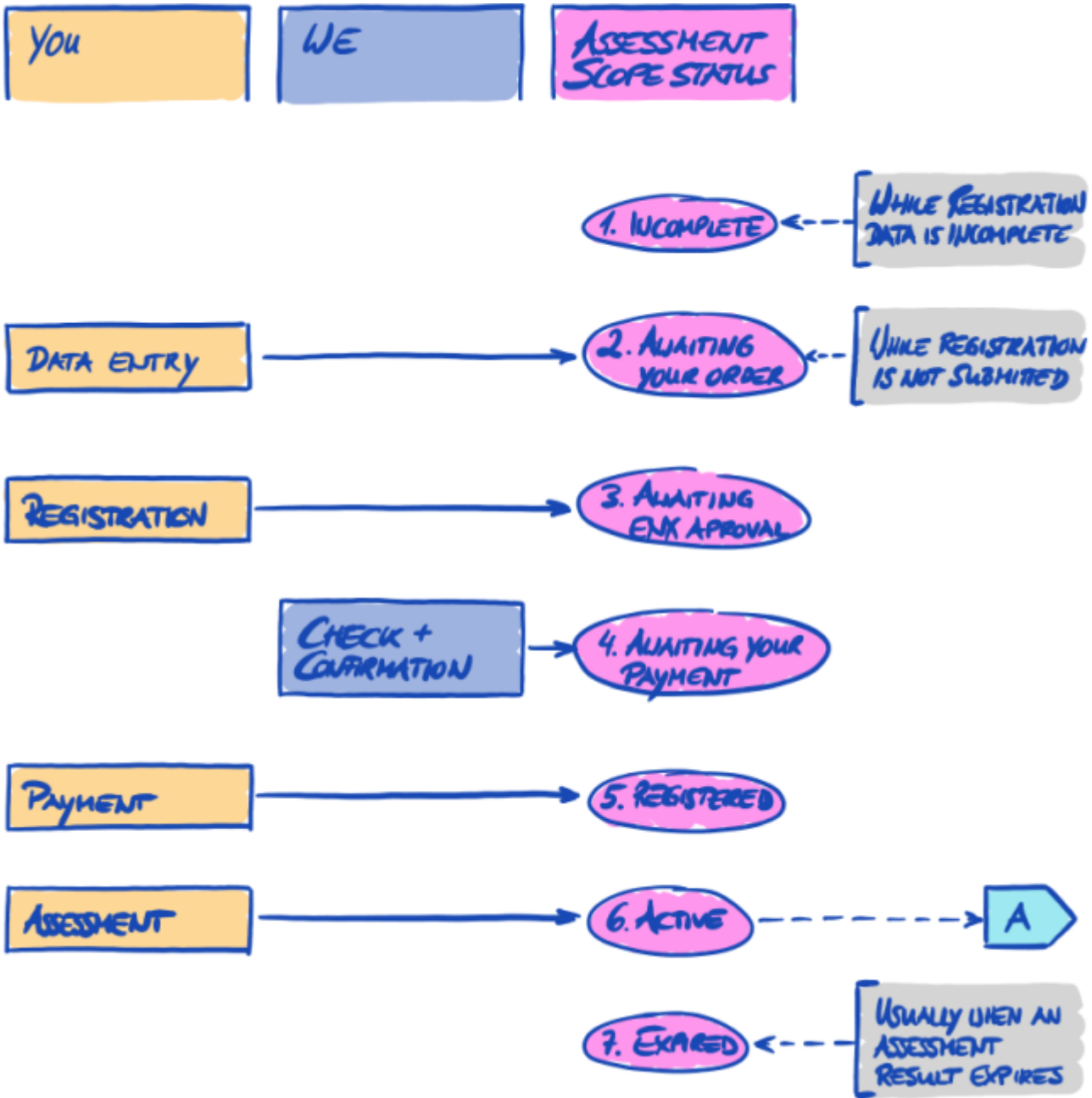


Figure 38. Assessment scope status overview

The off-page reference “A” in the figure above links the assessment scope status “Active” with the “assessment status”. For more information on the “assessment status”, please refer to Section 7.6, “Annex: Assessment status”.

7.5.2. Assessment scope status “Incomplete”

Status	Situation	Your next action	Our next action	Next status
Incomplete	Either you have not completed the assessment scope registration. Or you have not provided all the required information.	Continue at enx.com/en-US/SignIn	We will send you a reminder by email (usually within a few days).	Awaiting your order

For more information on where this status is playing a role, please refer to Section 4.5.7, “Assessment scope registration”.

7.5.3. Assessment scope status “Awaiting your order”

Status	Situation	Your next action	Our next action	Next status
Awaiting your order	You have not finished your scope registration.	Continue at  enx.com/en-US/SignIn	We will send you a reminder by email (usually within a few days).	Awaiting ENX approval

For more information on where this status is playing a role, please refer to Section 4.5.7, “Assessment scope registration”.

7.5.4. Assessment scope status “Awaiting ENX approval”

Status	Situation	Your next action	Our next action	Next status
Awaiting ENX approval	Your assessment scope registration is complete.	Wait for our next action.	We will check and typically approve your application. We will assign the Scope ID(s). We will send you a confirmation email. The attached “TISAX Scope Excerpt” (PDF) summarises the information we have in our database.	Awaiting your payment

For more information on where this status is playing a role, please refer to Section 4.5.7, “Assessment scope registration”.

7.5.5. Assessment scope status “Awaiting your payment”

Status	Situation	Your next action	Our next action	Next status
Awaiting your payment	Your assessment scope registration is complete and approved. You have received our confirmation email and the “TISAX Scope Excerpt”.	<p>Pay the fee (if applicable). Request offers from our TISAX audit providers. From the status “Awaiting your payment” onwards, you:</p> <ul style="list-style-type: none"> ▪ can start sharing some assessment-related information with your partner.^[34] ▪ can pre-configure the publication of your assessment result (this will only become effective once your assessment scope status changes to “Active”). <hr/> <p>34. While at assessment scope status “Awaiting your payment” or “Registered”, “Assessment Related information” includes assessment scope location(s), assessment scope status and assessment objective(s). It doesn’t include assessment results or TISAX labels.</p>	Waiting for your payment.	Registered

For more information on where this status is playing a role, please refer to Section 4.5.8, “Confirmation email”.

7.5.6. Assessment scope status “Registered”

Status	Situation	Your next action	Our next action	Next status
Registered	Your assessment scope is registered. We received your complete payment or your commercial status is “green” due to other circumstances.	Go through the TISAX assessment process.	None	Active

7.5.7. Assessment scope status “Active”

Status	Situation	Your next action	Our next action	Next status
Active	You have successfully completed the TISAX assessment process and received TISAX labels.	Publish and share your assessment result. Any publications and sharing permissions pre-configured at a lower status now become effective.	None	Expired

For more information on publishing and sharing, please refer to Section 6, “Exchange (Step 3)”.

7.5.8. Assessment scope status “Expired”

Status	Situation	Your next action	Our next action	Next status
Expired	Either: <ul style="list-style-type: none"> ▪ you have not completed your assessment scope registration within 90 days, ▪ or there has been an undue delay with your payment of the fee, ▪ or you have exited the TISAX process, ▪ or the validity of your assessment result has expired (three years), ▪ or you had major changes to the assessment scope (example: none of the locations in an assessment scope belong to your company any more). 	Start a new assessment scope registration.	None	Incomplete or Awaiting your order or Awaiting ENX approval

7.6. Annex: Assessment status

7.6.1. Overview: Assessment status

The “assessment status” defines where you are in the assessment process. The status changes with your progression from one assessment type to the next (like “initial assessment” to “corrective action plan assessment”).

Please be aware that the “assessment status” is different from the “assessment scope status”. For more information on the “assessment scope status”, please refer to Section 7.5, “Annex: Assessment scope status”.

Your “assessment status” can be:

1. Initial assessment ordered
2. Initial assessment ongoing
3. Waiting for corrective action plan assessment
4. Waiting for follow-up

5. Finished

The tables in each status' section below describe:

- your situation
(what's true right now when you are at this status)
- your next action
(what you need to do to progress to the next status; if applicable)
- our next action
(what we need to do to elevate your status; if applicable)
- the next status
(if applicable)

The following illustration shows the actions that lead to progress from one status to the next:

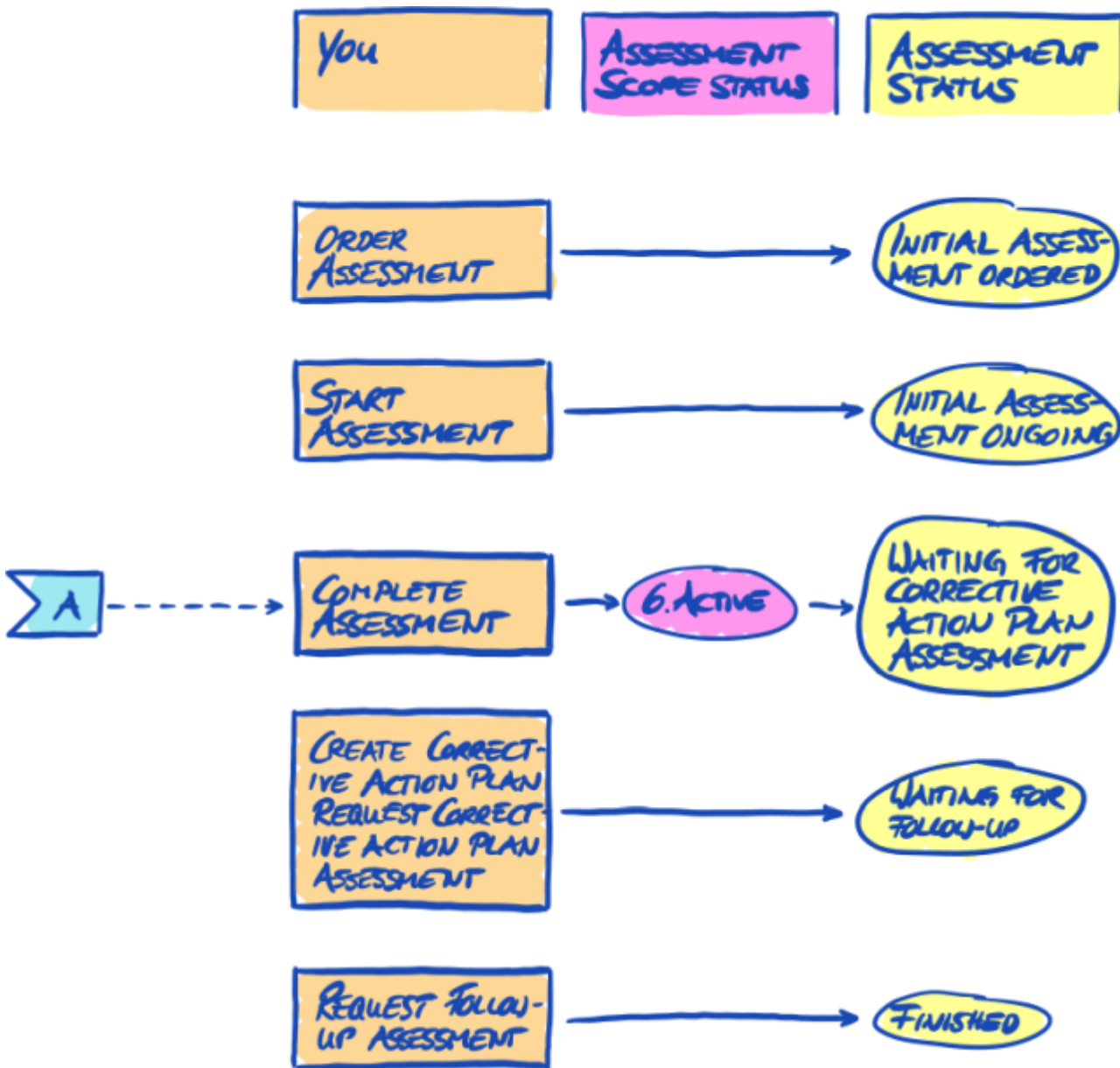


Figure 39. Assessment status overview

The off-page reference “A” in the figure above links the assessment scope status “Active” with the assessment status “Waiting for corrective action plan assessment”. For more information on the “assessment scope status”, please refer to Section 7.5, “Annex: Assessment scope status”.

7.6.2. Assessment status “Initial assessment ordered”

Status	Situation	Your next action	Our next action	Next status
Initial assessment ordered	You have selected one of our TISAX audit providers and ordered an initial assessment.	Continue the TISAX assessment process.	None	Initial assessment ongoing

7.6.3. Assessment status “Initial assessment ongoing”

Status	Situation	Your next action	Our next action	Next status
Initial assessment ongoing	Your initial assessment has either: <ul style="list-style-type: none"> ▪ started ▪ or is completed, but your audit provider has not yet submitted the TISAX assessment report 	None	None	Waiting for corrective action plan assessment (if applicable)

7.6.4. Assessment status “Waiting for corrective action plan assessment”

Status	Situation	Your next action	Our next action	Next status
Waiting for corrective action plan assessment	Your audit provider has conducted an initial assessment. Your audit provider has submitted the TISAX assessment report to us. The assessment result is (major/minor) non-conform.	Create a corrective action plan. Start the corrective actions. Request a corrective action plan assessment.	None	Waiting for follow-up (if applicable)

The assessment status “Waiting for corrective action plan assessment” is limited to nine months. For more information, please refer to Section 5.4.9.3, “Corrective action plan requirements”.

7.6.5. Assessment status “Waiting for follow-up”

Status	Situation	Your next action	Our next action	Next status
Waiting for follow-up	Your audit provider approved your corrective action plan. You have implemented the corrective actions.	Request a follow-up assessment.	None	Finished

The assessment status “Waiting for follow-up” is limited to nine months. For more information, please refer to Section 5.4.9.3, “Corrective action plan requirements”.

7.6.6. Assessment status “Finished”

Status	Situation	Your next action	Our next action	Next status
Finished	Your audit provider conducted a follow-up assessment. The assessment result has no non-conformities. Your audit provider submitted the TISAX assessment report to us.	Publish and share your assessment result.	None	n/a

7.7. Annex: The reasoning against “pre-assessments” and “gap analyses”

We generally advise against asking an audit provider to conduct a “pre-assessment” or a “gap analysis”. In almost all cases it makes more sense to start the TISAX assessment process right away.

In this section we address the most common concerns.

Do you consider a pre-assessment because:

1. You are concerned that your customer might see a potentially unfavourable assessment result?

You have full control over who sees your assessment results. It is your decision whether the audit provider uploads anything to the ENX portal. If no one should see it, no one sees it (except the auditor, of course).

Besides, the audit provider always only uploads the first two sections of the TISAX assessment report and *never* uploads the detailed assessment results anyway.

2. You think a pre-assessment might save money?

- With a pre-assessment, you:
 - pay for the pre-assessment
 - may have the internal costs of fixing any non-conformities
 - pay for the full TISAX assessment (“initial assessment”)

Even if there are *no* findings, you always pay for *two* full assessments.

- Starting with a TISAX assessment, you:
 - pay for the “initial assessment”
 - may have the internal costs of fixing any findings
 - may pay a lot less (compared to the initial assessment) for the so-called “follow-up assessment”, where the auditor only focusses on whether you fixed the non-conformities from the initial assessment

Even *with* findings, you only pay for a full assessment plus the short follow-up assessment.

3. You think you could fail the assessment with permanent consequences?

You can't permanently fail, because you can have as many assessments as you want. If the assessment result doesn't meet your expectations or if you fail to fix the non-conformities with corrective actions within the required nine month time period, you simply consider the failed attempt as your pre-assessment and start anew. And no one has to see the results of your first attempt. You just share the assessment result of the successful assessment.

Further considerations:

- If the assessment result is better than expected, you may receive temporary TISAX labels. You could directly share those with your partner. This is not possible with a pre-assessment.
- If the audit provider who conducts the pre-assessment should also conduct the TISAX assessment, he can't consult you. Otherwise, you have to choose another audit provider for the TISAX assessment.

While most auditees don't benefit from a pre-assessment, we want to mention the following advantages.

The auditor:

- can focus on critical aspects where you lack confidence in your ISMS
- can spend more time than usual and increase the insights
- can document findings differently

After reading the sections about the TISAX assessment process, it will be even easier for you to understand our reasoning.

7.8. Annex: Custom scopes

Almost all TISAX participants choose the standard scope. However, in certain and *rare* circumstances you may need to choose a custom scope.

There are two types of custom scopes:

7.8.1. Custom extended scope

You can extend the scope. A custom extended scope contains MORE than the standard scope. The audit provider will perform more checks.

Purpose: A custom extended scope may be relevant if you want to use your TISAX assessment for internal purposes or outside of the automotive industry.

TISAX labels and sharing results: A custom extended scope always includes the standard scope. Therefore, a custom extended scope will receive TISAX labels^[35]. Other TISAX participants will still accept the assessment result.

Description: While the standard scope has a predefined description, you need to write your own scope description if you need a custom extended scope.

7.8.2. Full custom scope

You can fully define your own scope.

Purpose: If you have locations that belong to different assessment scopes and that use services at a particular site (such as a data centre), you may use a full custom scope for those services. Thus, a TISAX audit provider can easily reuse the assessment result of the service's full custom scope.

Example: You have many locations (possibly part of different scopes) and you have a central IT department at one of those locations. Defining a full custom scope just for the IT department may make it easier to reuse the respective assessment result in the other scopes.

TISAX labels and sharing results: Full custom scopes don't receive TISAX labels. Your assessment result is recorded in the ENX portal with the date, validity period and whether the overall assessment result is conform or non-conform. You could share such an assessment result. But sharing an assessment result without TISAX labels will look like a "failed" assessment to most recipients. Other TISAX participants generally don't accept assessment results of full custom scopes.

Description: As for the custom extended scope, you need to write your own scope description if you need a full custom scope.



Important note:

To emphasize how rare the use of full custom scopes is: There is a 98% chance that your audit provider will revert your full custom scope to a standard scope. No participant *ever* successfully chose a full custom scope without advice from his audit provider.

An assessment with a full custom scope won't receive TISAX labels. We therefore generally advise against choosing a full custom scope — mainly because other participants generally don't accept assessment results with full custom scopes.

Do not choose a full custom scope if you don't have the explicit confirmation that your partner will accept the result and agreed with your particular scope description.

7.9. Annex: Participant data life cycle management

The following sections describe what you need to do if something related to your participant data changes.

7.9.1. Lost access to participant data (ENX portal)

If no one in your company who had access to the ENX portal and thus your participant data is left, please contact us. We will try to help you to regain access your company's participant data.


7.9.2. Administration of contacts

Your company's main participant contacts and all other "administrative contacts" with portal accounts can always go to the ENX portal and:

- add new contacts
- delete existing contacts
- change contact details of existing contacts


7.9.2.1. How to add a new contact

To add a new contact, follow these steps:

1. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “ADMINISTRATORS”.
4. Click the button “Create new TISAX Administrator”.
5. Enter the contact’s data.
6. Click the button “Save Contact”.
7. Go to the table and find the table row with the contact.
8. Go to the end of the table row of the contact and click the button with the down arrow .
9. Select “Edit TISAX Administrator”.
10. In the new window (“Edit TISAX Contact”), scroll down to the section “ENX PORTAL ACCESS”.
11. Select “Yes”.
12. In the appearing section “WEB ROLES”, click the button “Add Role”.
13. Select the role you want to assign (e.g. “TISAX Administrator”).
14. Click the button “Add Role”.
15. Click the button “Save Contact”.


7.9.2.2. How to delete an existing contact

To delete an existing contact, follow these steps:

1. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “ADMINISTRATORS”.
4. Go to the table and find the table row with the contact.
5. Go to the end of the table row of the contact and click the button with the down arrow .
6. Select “Delete TISAX Administrator”.
7. In the appearing confirmation request, click the button “Delete”.

7.9.2.3. How to update details of an existing contact

To update the details of an existing contact, follow these steps:

1. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “ADMINISTRATORS”.
4. Go to the table and find the table row with the contact.
5. Go to the end of the table row of the contact and click the button with the down arrow .
6. Select “Edit TISAX Administrator”.
7. Update the details.
8. Click the button “Save Contact”.

7.9.3. Administration of locations

Your company's main participant contacts and all other "administrative contacts" with portal accounts can always go to the ENX portal and request the:

- change of the company name
- change of a location (move/relocation)
- change of a street name
- addition of a new location

We describe the necessary steps in the following sections.



Please note:

- In TISAX, the combination of a company name and an address defines a "location".
- Each location has a "Location ID" (Location IDs always start with an "L" and are six characters long; Example: L1L3XY).
- If your company moves from its current address to a new address, the old location is no longer a valid location.



Important note:


Once you clicked the button "Save Location" in the ENX portal, you can't change it yourself anymore. For the situations described below, you can request changes.

7.9.3.1. How to request the change of your company name

Your situation: Your company has changed its name.

Example: The old company name is "ACME Tires Corporation".
The new company name is "ACME Corporation".

If you want to request the change of your company's name, please follow these steps:

1. Log in to the [ENX portal](https://enx.com/en-US/TISAX) (<https://enx.com/en-US/TISAX>).
2. Go to the main navigation bar and select "MY TISAX".
3. From the dropdown menu, select "LOCATIONS".
4. Go to the table and find the table row with your location.
5. Go to the end of the table row of your location and click the button with the down arrow .
6. Select "Request Change".
7. In the new window ("Request Change"), go to the form field "Subject of the change", open the dropdown menu and select "Company Name".
8. Continue filling out the form
9. Submit the form

We will check your request, possibly accept the request to change the company name, and inform you once it is done.

7.9.3.2. How to request the change of a location

Your situation: Your company moved to a new location.

Example: The old location is “ACME Corporation, **Bockenheimer Landstraße 97-99, 60325 Frankfurt, Germany**”.
The new location is “ACME Corporation, **Behrenstraße 35, 10117 Berlin, Germany**”.



Important note:

If an official authority renamed the street of your location, please refer to Section 7.9.3.3, “How to request the change of a street name” for more information.

If one of your locations relocated to a new address, please follow these steps:

1. Create a new location:

- a. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).
- b. Go to the main navigation bar and select “MY TISAX”.
- c. From the dropdown menu, select “Locations”.
- d. Click the button “Create TISAX Location”.
- e. In the new window (“CREATE TISAX LOCATION”), fill out the form with the details of the new location.
- f. Click the button “Save Location”.

2. Remember the “Location ID” of the newly created location. You can find the “Location ID” in the first column in the table “MY LOCATIONS”. Your audit provider needs the “Location ID” to update your assessment scope in the ENX portal.

3. Inform your audit provider about the relocation (provide the “Location ID” of the old location as well as of the new location).

Have you already completed the assessment?

- a. If the answer is NO, then there is nothing else to do for you regarding the change of the location.
- b. If the answer is YES, then you need to request a “scope extension assessment” from your audit provider. For more information, please refer to Section 7.10, “Annex: Scope extension assessment”.

The audit provider will check your request and update your assessment scope in the ENX portal.



Please note:

An audit provider can only update your assessment scope if you have already ordered the assessment from this audit provider.


7.9.3.3. How to request the change of a street name

Your situation: Your location’s street name has changed. Your company is still at the same physical site.

Example: The old location is “ACME Corporation, **Bockenheimer Landstraße 97-99, 60325 Frankfurt, Germany**”.
The new location is “ACME Corporation, **Behrenstraße 97-99, 60325 Frankfurt, Germany**”.

If an official authority renamed the street of your location, please follow these steps:

1. Log in to the [ENX portal](https://enx.com/en-US/TISAX/) (https://enx.com/en-US/TISAX/).

2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “Locations”.
4. Go to the table and find the table row with your location.
5. Go to the end of the table row of your location and click the button with the down arrow .
6. Select “Request Change”.
7. In the new window (“Request Change”), go to the form field “Subject of the change”, open the dropdown menu, and select “Address”.
8. Continue filling out the form
9. Submit the form

We will check your request, possibly accept the request to change the street name, and inform you once it is done.



Important note:

These steps only apply when your company is still at the same physical site, but an official authority changed the name of the street.

If you moved to a new location, please refer to Section 7.9.3.2, “How to request the change of a location” for more information.

7.9.3.4. How to add an additional location

If you open an additional location during the validity period of your existing TISAX labels, you can request a “scope extension assessment” from your audit provider.

For more information, please refer to Section 7.10, “Annex: Scope extension assessment”.

7.10. Annex: Scope extension assessment

Besides the standard assessment types described in Section 5.4.3, “TISAX assessment types”, there is another special assessment type: the “scope extension assessment”.

You can extend an existing TISAX assessment scope if want to add one or more:

- assessment objectives, or
- locations.

You can’t select another audit provider to conduct a “scope extension assessment”. The assessment is similar to the standard assessment types. However, your audit provider will most likely consider reusing applicable results from previous assessments.

Once the scope extension assessment is concluded without non-conformities, your audit provider will:

- update your assessment scope in the ENX portal.
- issue the scope extension assessment report.

A scope extension assessment does not extend the original validity period of your existing TISAX labels.



Please note:

If the reason for the scope extension assessment is either a relocation or an additional location, you have to create the new location in the ENX portal. Please provide the “Location Excerpt” or at least the “Location ID” to your audit provider.

Each location has a “Location ID” (Location IDs always start with an “L” and are six characters long; Example: L1L3XY). Your audit provider needs the Location ID to update your assessment result in the ENX portal.

7.11. Annex: ISA life cycle management

An ENX working group is maintaining the ISA.

These facts may be of interest to you:

- The VDA officially publishes new versions.
- The audit provider will use the ISA version that is valid when you *order* your initial assessment
- By mutual agreement, you can use a newer ISA version if one is published between your order and the start of the initial assessment.
- You can find the publication date of a given ISA version in the Excel sheet “Cover”.
 - Example:
Version: 5.0 | Revision 4 | 2021-04-16

7.12. Annex: Helpful documents

This section lists documents we consider helpful.

- Whitepaper “Harmonization of classification levels”

“This White Paper describes the Information security working group’s proposal for determining a scheme focusing on the protection objective of confidentiality; this means that information is not made accessible to unauthorized persons, organizations or processes. Additionally, the protection objectives such as availability, integrity and reliability are not the focus of this White Paper.”

Available languages: English

Publisher: Verband der Automobilindustrie e.V. (“German Association of the Automotive Industry”)

 www.vda.de/en/news/publications/publication/harmonization-of-classification-levels

- White Paper “Information Security Risk Management”

“The objective of this White Paper is to inform companies in the automotive industry with regard to risk-oriented information security management and to enable those to establish an effective information security risk management. It is intended to support organizations in preparing or conducting a TISAX assessment to meet the requirements of the VDA ISA control question 1.4.1. It’s content it is to be considered as implementation recommendations, not as a mandatory requirements.”

Available languages: German, English

Publisher: Verband der Automobilindustrie e.V. (“German Association of the Automotive Industry”)

 <https://www.vda.de/en/news/publications/publication/white-paper-information-security-risk-management->

7.13. Annex: Complaint management

7.13.1. Causes for complaint

Our complaint management differentiates between these two areas:

1. ENX Association — the organisation that governs TISAX
2. Audit providers — the organisations that conduct the TISAX assessments

7.13.1.1. Complaints about ENX Association

If you have a complaint about ENX Association, please contact our “TISAX manager on duty” (see contact details below).

7.13.1.2. Complaints about audit providers

First, you should try to solve the issue directly with the auditor.

The next step should be the person responsible for TISAX at the audit provider.

Thereafter, your next contact would be the person responsible for the audit provider’s quality management.

If the issue is still unsolved, you should contact our “TISAX manager on duty” (see contact details below).

There are even options above the “TISAX manager on duty”. In such cases, you would talk to ENX Association’s managing director.

The VDA has no role in the complaint management.



Please note:

The audit provider must inform you about your right to complain during the kick-off meeting. If he doesn’t, this would already be a reason for a complaint.

7.13.1.3. Requirements for complaints

If you want to involve us, we need the following information:

- Who is complaining?
 - Company name
 - TISAX Participant ID
 - Contact (name, email address, phone number)
- Which assessment is it?
 - Assessment ID
 - If the assessment is not yet recorded in the ENX portal: Scope ID
- Who is the audit provider?
 - Audit provider company name
 - Name of the auditor(s)
- What are you complaining about?
 1. General complaint about the performance of the audit provider
 2. Complaint about the approach of the auditor

3. Complaint about the assessment with regards to content

- For complaints about the assessment with regards to content: Which finding do you object?
 - Control (e.g. 1.6.1 "To what extent are information security events processed?")
 - Finding (full text)
 - Objection against:
 - Interpretation of the control
 - Ascertainment with regards to content (available evidence is not assessed correctly)
 - Risk assessment (appropriateness not considered)
- Reasoning why you assess things differently



7.13.2. Contact for complaints

Please contact the "TISAX manager on duty":

Send him an email at: tisax-complaints@enx.com

Or call him at: [+49 69 9866927-79](tel:+4969986692779)

You can reach him during regular business hours in Germany (UTC+01:00
(https://www.worldtimeserver.com/current_time_in_DE.aspx)).

He speaks  English and  German.

8. Document history

Version	Notes
2.5.1	<ul style="list-style-type: none"> ▪ Broken links fixed
2.5	<ul style="list-style-type: none"> ▪ Section "Administration of locations" added ▪ Section "Annex: Helpful documents" updated to reflect changes in the links

Version	Notes
2.4	<ul style="list-style-type: none"> ▪ Imprecise statement regarding the maximum duration of the TISAX assessment process removed from Section 3.1, “Overview” ▪ “TISAX report” renamed to “TISAX assessment report” ▪ Note regarding the differences between ISO 27001 and TISAX updated ▪ Section “Scope description” updated; custom scope section moved to annex ▪ “Standard scope description” updated to version 2.0 ▪ Section “Publication and sharing” updated with note about sharing the assessment status ▪ Section “Protection needs and assessment levels” updated with content about “assessment level 2.5”, the “video-supported remote assessment method”, the differences between AL 2 and AL 3, plausibility check vs. verification ▪ Link to the start of the registration process updated ▪ Section “Portal account” updated to reflect the changed invitation process ▪ Download links to the ISA document changed (now also available on enx.com) ▪ Section “Evaluating offers” updated with a basis for cost estimates ▪ Section “Kick-off meeting” added (with content moved here from section “The first formal opening meeting”) ▪ Section “About conformity” updated with a new table about the four types of findings ▪ Section “Initial assessment” updated with note regarding time constraints ▪ Section “TISAX assessment report” updated with note regarding a pro-active corrective action plan ▪ Section “Corrective action plan preparation” updated with the requirements “finding” and “root cause” and a note regarding corrective action plan templates ▪ Section “Corrective action plan assessment” updated with a remark regarding email as the sole communication mode ▪ Section “Prerequisites for a corrective action plan assessment” renamed to “Reasons for a corrective action plan assessment” and two reasons added ▪ Section “Temporary TISAX labels” updated with examples and clarifications regarding the validity period ▪ Section “TISAX report” renamed to “TISAX assessment report” ▪ Section “Renewal of TISAX labels” updated with note regarding the reuse of location records in the ENX portal ▪ Section “Annex: The reasoning against “pre-assessments” and “gap analyses”” added ▪ Section “Annex: Custom scopes” added (“Extended scope” and “Narrowed scope” replaced with “Customer extended scope” and “Full custom scope”) ▪ Section “Annex: Scope extension assessment” updated with reasons and a note regarding adding location records to the participant’s ENX portal account ▪ Section “Annex: ISA life cycle management” updated to reflect the current situation ▪ Section “Annex: Helpful documents” updated to reflect changes in the links

Version	Notes
	<ul style="list-style-type: none"> ▪ Section “Annex: Complaint management” added ▪ Phone numbers are now clickable ▪ Various minor clarifications and small corrections ▪ Minor typing errors corrected ▪ Note for TISAX audit providers: This update is based on ENX doc ID 612 version 2.1
2.3	<ul style="list-style-type: none"> ▪ Subtitle reworded ▪ Change from Word/PDF to HTML as the primary format for the handbook ▪ Further translations available (Chinese and French, see next bullet point) ▪ Section “The TISAX participant handbook in other languages and formats” added ▪ All links to the ENX homepage changed from "https://portal.enx.com" to "https://enx.com" (the old links still work) ▪ “VDA ISA” becomes “ISA” ▪ Section Section 5.2, “Self-assessment based on the ISA” updated to reflect changes introduced with ISA version 5 ▪ Rows of all tables listing assessment objectives reordered to match the changed order of the criteria catalogs in ISA 5 ▪ Figures listing assessment objectives updated to match the changed order of the criteria catalogues ISA 5 ▪ Section “Scope tailoring” updated (figure 6, typing error corrected, assessment objectives updated) ▪ Section “Fee” updated with information about credit card payments ▪ Section “TISAX assessment process diagram” updated (figure 34, reference to managed service provider removed) ▪ Section “Annex: Helpful documents” updated (White Paper “Information Security Risk Management” added)
2.2.1	<ul style="list-style-type: none"> ▪ Minor typing errors corrected

Version	Notes
2.2	<ul style="list-style-type: none"> ▪ Cover printing issue fixed ▪ All links to our homepage and the downloads changed ▪ We now also speak Italian ▪ Section “Custom scope” extended ▪ Section “Scope locations” updated ▪ Assessment objectives “Connection to 3rd parties” removed; figures 7, 9, and 38 updated; tables 4, 5, 6, and 8 updated ▪ Wording “<i>with</i> assessment level” changed to “<i>in</i> assessment level” ▪ Reference to “TISAX activation list” in section “Protection needs and assessment levels” removed (no longer applicable) ▪ Section “Assessment objectives and your own suppliers” added ▪ Section “Participant contact” updated with information regarding group email addresses and inviting contacts to allow them to manage participant data in the ENX portal ▪ Section “Assessment scope registration” updated with information about changes to the assessment scope ▪ Section “Status information” updated (figure 12) ▪ Section “Address the self-assessment result” updated with information regarding external help by third parties ▪ Section “Coverage” updated with link to audit provider coverage matrix ▪ Section “Requesting offers” updated ▪ Section “Evaluating offers” updated with information regarding “pre-assessments” ▪ Section “Renewal of TISAX labels” updated with information regarding the need to register a new scope ▪ Various sub-sections of section “Exchange (Step 3)” updated to reflect interface changes in the ENX portal ▪ Section “Share your assessment result with a particular partner” updated with recommendation regarding the sharing level and note regarding automated processing of shared assessment results ▪ Section “Sharing your assessment result outside TISAX” added ▪ Section “ISA lifecycle management” added ▪ Section “Annex: Assessment scope status” updated (new status “Awaiting your order”, status “Awaiting approval” renamed to “Awaiting ENX approval”, status “Approved” renamed to “Awaiting your payment”, figure 40) ▪ Section “Annex: Example confirmation email” updated ▪ Section “Annex: Example TISAX Scope Excerpt” updated ▪ Section “Annex: Assessment status” updated (new status “Initial assessment ongoing”, status “Waiting for follow-up assessment” renamed to “Waiting for follow-up”, figure 41) ▪ Section “Annex: Volkswagen legacy assessments” (and references to it) removed (no longer relevant)

Version	Notes
2.1.2	<ul style="list-style-type: none"> ▪ Formal limit for “distance” between “your result score” and “maximum result score” corrected from 25% to 30%
2.1.1	<ul style="list-style-type: none"> ▪ Minor typing errors corrected
2.1	<ul style="list-style-type: none"> ▪ Section “Managed Service Providers” removed ▪ New TISAX assessment objectives / labels (data protection labels based on GDPR; four instead of two prototype labels; Renaming: protection needs instead of protection levels; selection advice updated) ▪ Updates due to changes in the ISA (version 4.0 to 4.1) ▪ Reference to the new document “TISAX Simplified Group Assessment” (addendum to this handbook) ▪ Suggestions for assigning location names and scope names added ▪ “Registration fee” renamed to “fee” ▪ Recommendation for contact deputies added ▪ Selection of charging model removed

Back to top.

1. You may want to consider going through the TISAX process as a pre-emptive step. Some companies do this in order to be better prepared. Already being TISAX-assessed may mean a much shorter onboarding period and therefore may give you an edge over not-yet-TISAX-assessed competitors.
2. “TISAX labels” are a concept to summarise your assessment result and are the output of the TISAX process. Please refer to Section 5.4.14, “TISAX labels” for more details.
3. You only need to take most of registration steps once when you start as a TISAX participant. When you renew your assessment result, you only need to update and confirm your registration data.
4. We will publish changes to our GTCs on the ENX portal and notify registered contacts.
5. This also applies to all other additional agreements (e.g. codes of conduct).
6. Please note that currently your partner is not automatically informed about new permissions. You may want to notify your partner once your assessment result is available to him.
7. If you want to be on that list, please contact us.
8. Evidence is anything that supports your assertion that you fulfil a certain requirement. Evidence is mostly documents. You will surely use internal documentation as evidence.
9. Interviews for assessments with assessment level 2 are generally conducted via web conference. At your request, interviews can be conducted on site
10. The theoretical minimum for simplified group assessments is three locations.
11. If you already know you will have to improve your information security management system, the recommended minimum is at least twelve locations.
12. To prevent possible confusion between numbers and letters (like 8 and B), certain letters are not allowed in Participant IDs. However, some older Participant IDs may contain the letter “G”.
13. The ISA also refers to the criteria catalogues as “modules”.
14. You can find the underlying Excel feature in the ribbon “Data”, section “Outline”.
15. Do you have audit providers for your company for similar assessments (like ISO 27001) that are interested in conducting TISAX assessment as well? Then share this handbook with them and tell them to contact us
16. Audit providers that are not included in our listing are not allowed to conduct TISAX assessments.
17. If you end the assessment process, you won’t receive TISAX labels.
18. There is actually a fourth type: The “scope extension assessment”. As this is a special case, it is described in detail in the annex in Section 7.10, “Annex: Scope extension assessment”.

19. The formal *opening* meeting will be described in detail for the initial assessment only. For the other TISAX assessments, your audit provider will schedule and shape these meetings.
20. Some audit providers may use the term “kick-off meeting” synonymously for “formal opening meeting”.
21. The formal *closing* meeting will be described in detail for the initial assessment only. For the other TISAX assessments, your audit provider will schedule and shape these meetings.
22. If a dispute can't be solved, you can escalate the issue. For more information, please refer to Section 7.13, “Annex: Complaint management” for further details.
23. For more information on audit methods and intensities, please refer to Section 4.3.3.6, “Protection needs and assessment levels”.
24. If a dispute can't be solved, you can escalate the issue. Please contact us for further details.
25. Please note that your overall assessment result can still be “major non-conform”, even if you have defined appropriate corrective actions. This is the case if your measures don't/can't immediately take effect.
26. This of course only applies to an initial assessment that identified non-conformities. You don't need a follow-up assessment for an initial assessment with an assessment result of “conform”.
27. In theory, this can be nine month after the conclusion of the initial assessment.
28. Actually, there is a fourth type: The “scope extension assessment report”. As this is a special case, it is described in detail in Section 7.10, “Annex: Scope extension assessment”.
29. The “TISAX assessment report” is based on a template that all TISAX audit providers are obliged to use.
30. The word “renewal” can be misleading. To keep a TISAX label for more than three years, you need to run through the TISAX process again. This starts with registering a new assessment scope.
31. We don't maintain a “TISAX-public” list of Participant IDs. The reason for this is that we want to prevent accidental sharing based on similar-sounding company names or other “human errors”. Therefore, you always have to obtain your partner's Participant ID by contacting him directly.
32. Your partner has to log into the portal and actively look up your shared assessment result. Your partner doesn't receive an automated notification about new shared assessment results.
33. The rule is defined in the “TISAX Participation General Terms and Conditions” (<https://enx.com/tisaxgtcen.pdf> (<https://enx.com/tisaxgtcen.pdf>)).
35. “TISAX labels” are a concept to summarise your assessment result and are the output of the TISAX process. Please refer to Section 5.4.14, “TISAX labels” for more details.

[About us](https://enx.com/en-US/enxassociation/) (<https://enx.com/en-US/enxassociation/>)

[Contact](https://enx.com/en-us/contact/) (<https://enx.com/en-us/contact/>)

[Legal notice](https://enx.com/en-us/imprint/) (<https://enx.com/en-us/imprint/>)

[Privacy policy](https://enx.com/en-US/data-protection/) (<https://enx.com/en-US/data-protection/>)