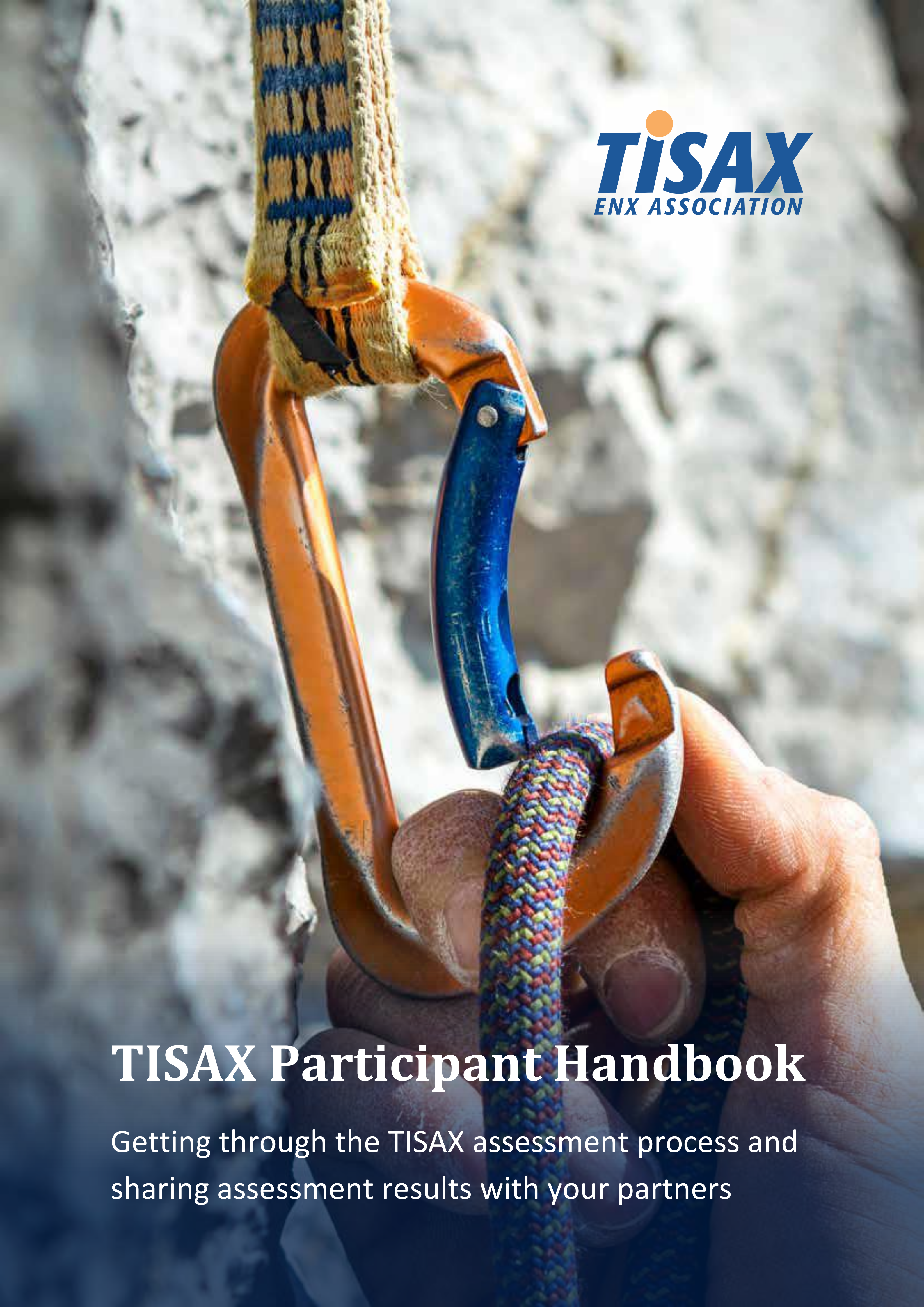


TISAX
ENX ASSOCIATION

TISAX Participant Handbook

Getting through the TISAX assessment process and sharing assessment results with your partners

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: 2019-09-17, Version: 2.1.2

Classification: Public, ENX doc ID: 602

Copyright notice

Table of contents

List of tables

List of figures

1 Overview

1.1 Purpose

Welcome to TISAX, the Trusted Information Security Assessment Exchange.

One of your partners requested that you prove your information security management complies with a defined level according to the requirements of the “VDA[1] Information Security Assessment” (VDA ISA). And now you want to know how to fulfil this request.

The very purpose of this handbook is to enable you to fulfil your partner's request – or to have an edge by anticipating it before any partner asks for it.

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

To establish and maintain 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 managing 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 run 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 “VDA Information Security Assessment” (VDA 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 start with instructions on HOW to do things. The primary focus in the first sections is on action-oriented content. You will find all you need to get through the process – in the order you need to know it.

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

[1] Verband der Automobilindustrie e. V. (VDA), https://www.vda.de

1.5 How to use this document

Sooner or later you will probably want to understand most of what is described in this document. For a proper preparation we recommend reading the entire handbook.

However, we structured the handbook along the three main steps of the TISAX process. Thus, you can pick the section you currently need and read the rest later.

The handbook uses illustrations to help you improve your understanding. Often, the colours in the illustrations carry supportive meaning. Therefore, we recommend either reading the document on a screen or as colour hard copy.

We appreciate your feedback. If you think anything 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.

Please note:

You can download the most current version of our handbook on our website at:

https://enx.com/tisax/tisax-en.html#registration ("TISAX Participant Handbook" in the column on the right)

Direct PDF download:

https://enx.com/tisax/files/downloads/TISAX-Participant-Handbook-current.pdf

If you already used a prior version to the TISAX participant handbook, you may find some helpful notes at the end of the document in the section "8 Document history" on page 100.

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 give us a call at: +49 69 9866927-77

You can reach us during regular business hours in Germany (UTC+01:00).

We speak English and German.

1.7 The TISAX handbook in other languages

The TISAX handbook is also available in German.

You can download the German version on our website at:

https://enx.com/tisax

Direct PDF download:

https://enx.com/tisax/files/downloads/TISAX-Teilnehmerhandbuch.pdf

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” on page 16.

2.1 Why TISAX?

Or rather, why are you here?

For answering this question, we start with some general 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. Thus, 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?

Neither your partner nor you are 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.

Every time you would have to independently create a solution for a common problem, a standard way of doing it takes off the burden of creating everything from scratch. While defining a standard is a huge effort, it is made only once and the followers 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, ISMS) and their implementations establish a state-of-the-art way of how to securely handle confidential information. Such a standard saves you from having to reinvent the wheel. More important, standards provide a common basis when two companies need to exchange confidential data.

2.3 The automotive way

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

Already a long time ago, the automotive industry formed associations whose aims are – among others – to refine and define standards that care for their more specific needs. The “Verband der Automobilindustrie” (VDA) is one of them. Within 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.

The result of their joint efforts is a questionnaire that covers the automotive industry's widely accepted information security requirements. It is called the “VDA Information Security Assessment” (VDA ISA).

With the VDA 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 VDA ISA just for internal purposes, others use it to assess the maturity of the information security management of their suppliers. In some of those cases a “self-assessment” was a sufficient basis for the business relationship. For certain cases however, companies conducted a complete assessment of their supplier's information security management (including on-site audits).

Along with a generally increasing awareness of the need for information security management and the spreading adoption of the VDA 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 styles.

And the more suppliers were requested by their partners to prove their level of information security management, the louder the voices grew that complained about repeated efforts. Showing one auditor after the other 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?

The OEMs and suppliers in the VDA working group that is responsible for maintaining the VDA ISA listened to their supplier's complaints. Now they offer an answer for their suppliers as well as for 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[2] starts with one of your partners requesting you to prove a defined level of information security management according to the requirements of the "VDA Information Security Assessment" (VDA 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:

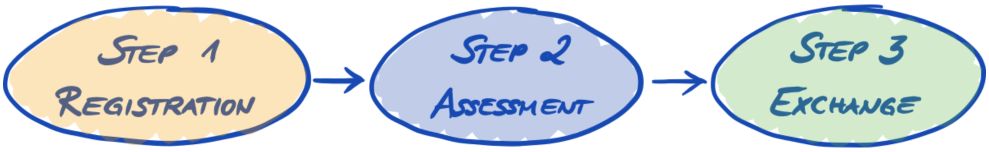


Figure 1: TISAX process overview

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

However, TISAX defines a maximum duration of nine months for the entire TISAX assessment process.

[2] 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 thus may give you an edge over not-yet-TISAX-assessed competitors.

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)” on page 15.

The online registration process is described in detail in section “4.5 Online registration process” on page 38. But if you want to start right away, please go to 🇬🇧 https://enx.com/tisax/tisax-en.html#registration.

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. To which extent depends on the current maturity level of your information security management system. But your preparation has to be based on the VDA ISA catalogue.

b) Audit provider selection

Once you are ready for the assessment, 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 at least consist of the initial audit.

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

d) Assessment result

Once your company passed the assessment, your audit provider will provide you the official TISAX report. Your assessment result will also receive TISAX labels[3].

For more information about this step, please refer to section “5 Assessment (Step 2)” on page 47.

3.4 Exchange

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

[3] “TISAX labels” are a concept to summarize your assessment result and are the output of the TISAX process. Please refer to section “5.4.13 TISAX labels” on page 76 for more details.

Your assessment result is valid for three years. Assuming you are still a supplier of your partner then, you will have to renew your assessment result by following the 3-step process again[4].

For more information about this step, please refer to section “6 Exchange (Step 3)” on page 81.

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

[4] 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 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.

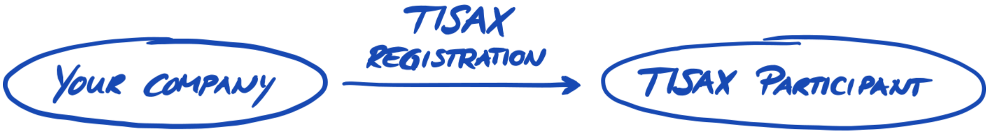


Figure 2: Register to become a TISAX participant

To reflect 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.

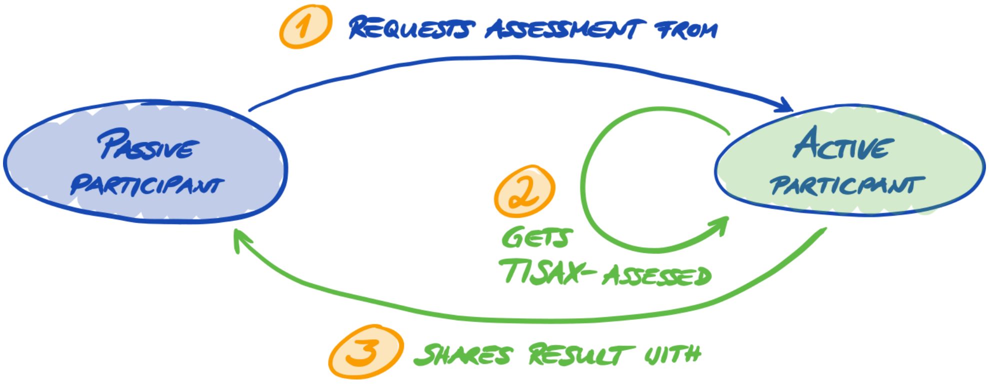


Figure 3: Passive participant and active participant

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.

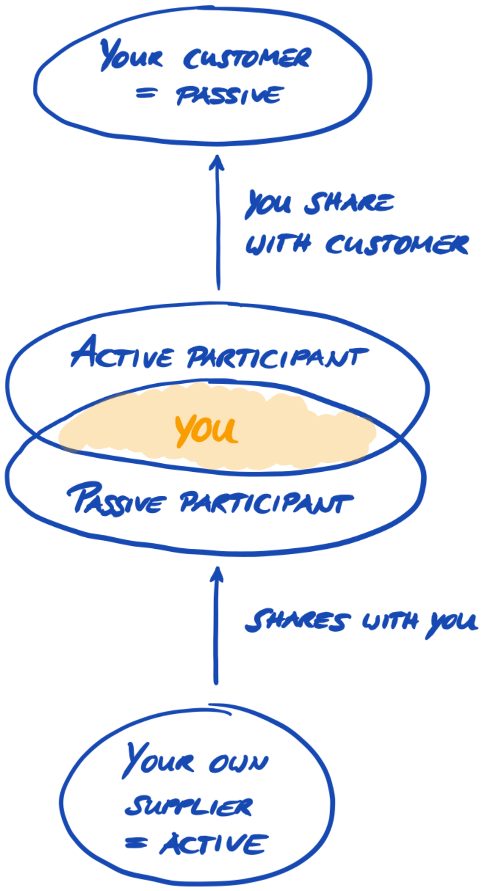


Figure 4: TISAX participants can be active and passive at the same time

Requesting your own suppliers to get TISAX-assessed may even be especially advisable if your own suppliers are handling your partner's confidential information, too.

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” on page 38.

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

- gathering some information in advance
- and already taking some decisions.

Please note:

If you are a partner of Volkswagen AG, Audi AG or Porsche AG, and if “operational services GmbH & Co. KG” started the assessment between the years 2015 and 2017, you can transfer your “Volkswagen legacy assessment result” to TISAX.

For instructions on how to trigger the transfer, please refer to section “7.8 Annexe: Volkswagen legacy assessments” on page 98.

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 only look at the first one.

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 internal or external lawyer.

You can download the "TISAX Participation General Terms and Conditions"[5] on our website at:

🇬🇧 https://enx.com/tisax/tisax-en.html#registration

Direct PDF download:

🇬🇧 https://enx.com/tisax/files/downloads/ENX-TISAX-Participation-GTCs-current.pdf

🇩🇪 http://www.enx.com/tisax/files/downloads/ENX-TISAX-Participation-GTCs-DE-EN-current.PDF

⚠ Important note:

The TISAX Participant GTCs are in English. A German translation is available, but during the online registration process you have to accept the English version.

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. 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, we kindly ask you to check the respective sections in our GTCs. They should address all your concerns.

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[6].

[5] We will publish changes of our GTCs on the ENX portal and notify registered contacts.

[6] This also applies to all other additional agreements (e.g. codes of conduct).

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. Simplified, every part of your company that handles confidential information of your partner 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:
If your company has an ISO/IEC 27001 certification: The definition of the "TISAX assessment scope" and the scope definition required for the ISO/IEC 27001 certification have a similar coverage. The difference is that in TISAX the scope is predefined.

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) Extended scope
    b) Narrowed scope

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. If for any reason you want to use a custom scope description, you can choose to either extend or narrow the scope of your assessment.

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[7]:

The standard 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.

Examples for involved resources: Work equipment, employees, IT systems including cloud services such as infrastructure/ platform/software as a service, physical sites, relevant contractors

Examples for sites: Office sites, development sites, production sites, data centres

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

4.3.2.3 Custom scope

The standard scope is what almost all TISAX participants choose. However, in certain circumstances you may need to choose a custom scope.

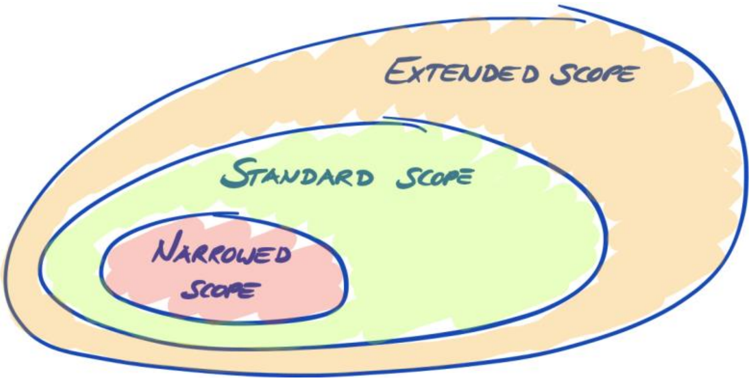


Figure 5: Scope types: extended scope, standard Scope, narrowed scope

a) Extended scope

You can extend the scope. An extended scope contains MORE than the standard scope. The audit provider will do more checks. This may be relevant if you want to use your TISAX assessment for internal purposes or outside of the automotive industry.

An extended scope always includes the standard scope. Other TISAX participants will still accept the assessment result.

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

b) Narrowed scope

You can narrow the scope. A narrowed scope contains LESS than the standard scope. The audit provider will skip certain checks.

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

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

[7] This is the standard scope description in version 1.0. We added versioning because we may update the description in the future.

Here is an example of a narrowed scope description:

Physical security, resources and processes of the part of the data centre that are used to fulfil services of Company X[8].

⚠ Important note:

An assessment with a narrowed scope won't receive TISAX labels[9]. We therefore generally advise against choosing a narrowed scope – mainly because other participants usually don't accept assessment results with narrowed scopes. Please consult your partner before choosing a narrowed scope.

4.3.2.4 Scoping

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

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

If your company is large, you should 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 like:

- 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.[10]

4.3.2.5 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.

[8] “X” is your company.

[9] “TISAX labels” are a concept to summarize your assessment result and are the output of the TISAX process. Please refer to section “5.4.13 TISAX labels” on page 76 for more details.

[10] 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.

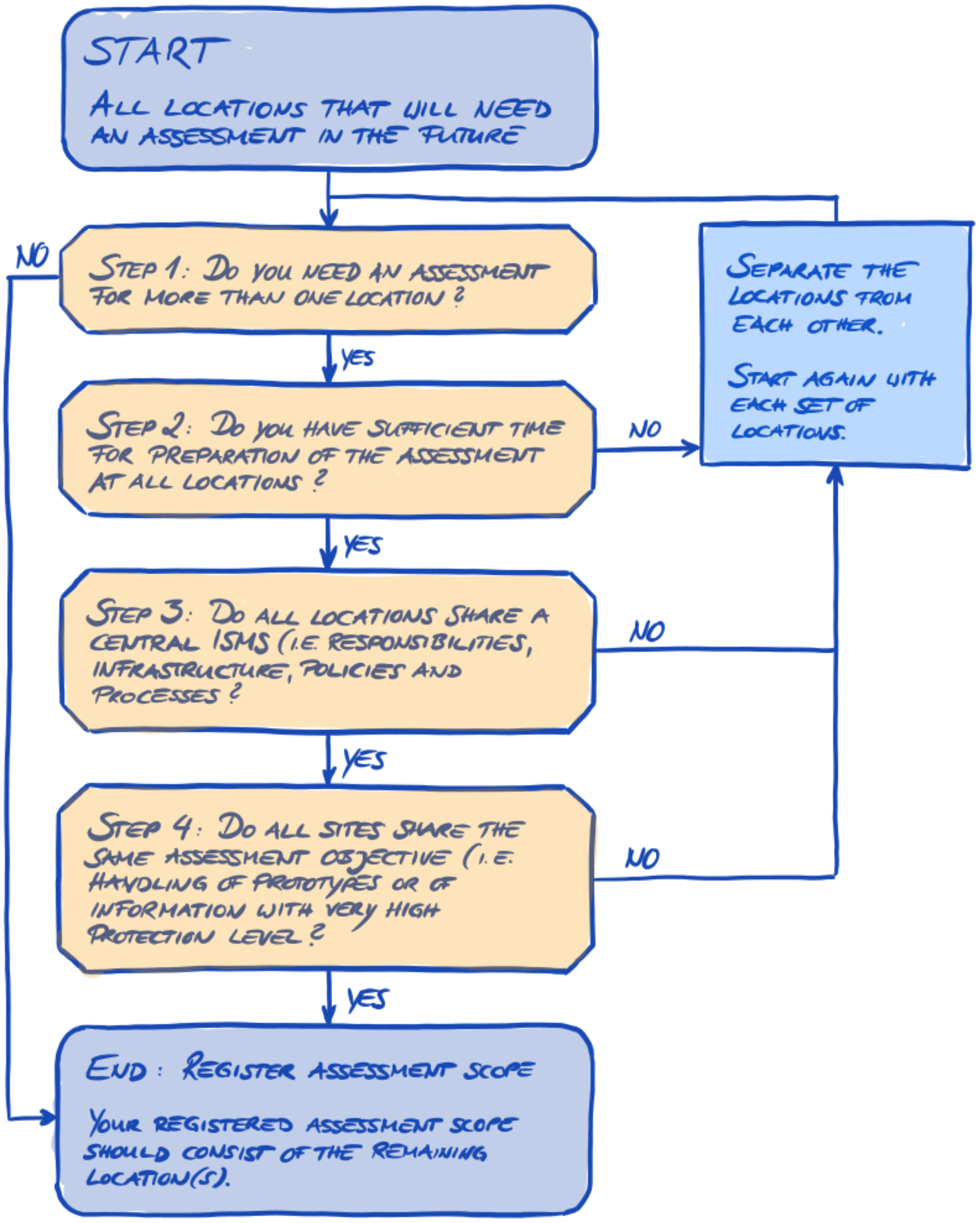

START
ALL LOCATIONS THAT WILL NEED AN ASSESSMENT IN THE FUTURE
STEP 1: DO YOU NEED AN ASSESSMENT FOR MORE THAN ONE LOCATION ?
NO
YES
STEP 2: DO YOU HAVE SUFFICIENT TIME FOR PREPARATION OF THE ASSESSMENT AT ALL LOCATIONS ?
NO
SEPARATE THE LOCATIONS FROM EACH OTHER.
START AGAIN WITH EACH SET OF LOCATIONS.
YES
STEP 3: DO ALL LOCATIONS SHARE A CENTRAL ISMS (I.E. RESPONSIBILITIES, INFRASTRUCTURE, POLICIES AND PROCESSES ?
NO
YES
STEP 4: DO ALL SITES SHARE THE SAME ASSESSMENT OBJECTIVE (I.E. HANDLING OF PROTOTYPES OR OF INFORMATION WITH VERY HIGH PROTECTION LEVEL ?
NO
YES
END: REGISTER ASSESSMENT SCOPE
YOUR REGISTERED ASSESSMENT SCOPE SHOULD CONSIST OF THE REMAINING LOCATION(S).

Figure 6: 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.

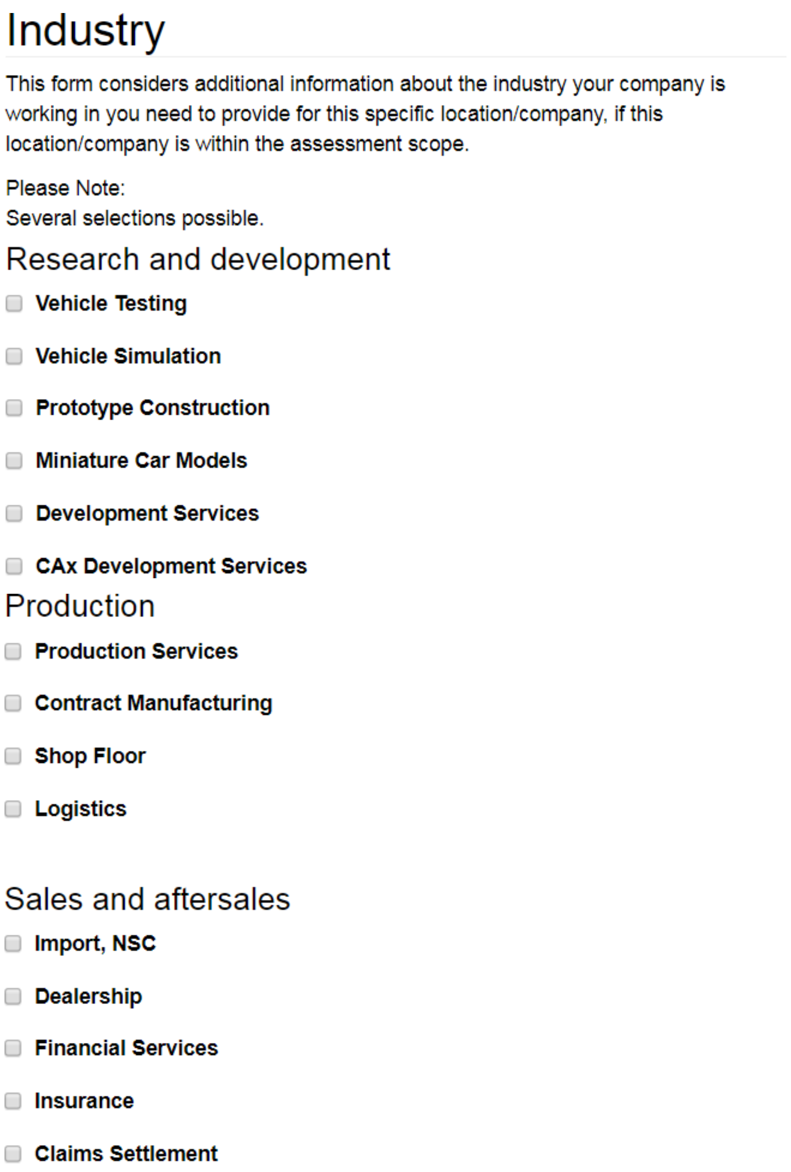
Please note: Adding to the scope increases the fee and you won't get a refund if you remove locations from the scope.

4.3.2.6 Scope locations

Now that you have decided which locations are parts 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:



Industry

This form considers additional information about the industry your company is working in you need to provide for this specific location/company, if this location/company is within the assessment scope.

Please Note:
Several selections possible.

Research and development

□ **Vehicle Testing**

□ **Vehicle Simulation**

□ **Prototype Construction**

□ **Miniature Car Models**

□ **Development Services**

□ **CAx Development Services**

Production

□ **Production Services**

□ **Contract Manufacturing**

□ **Shop Floor**

□ **Logistics**

Sales and aftersales

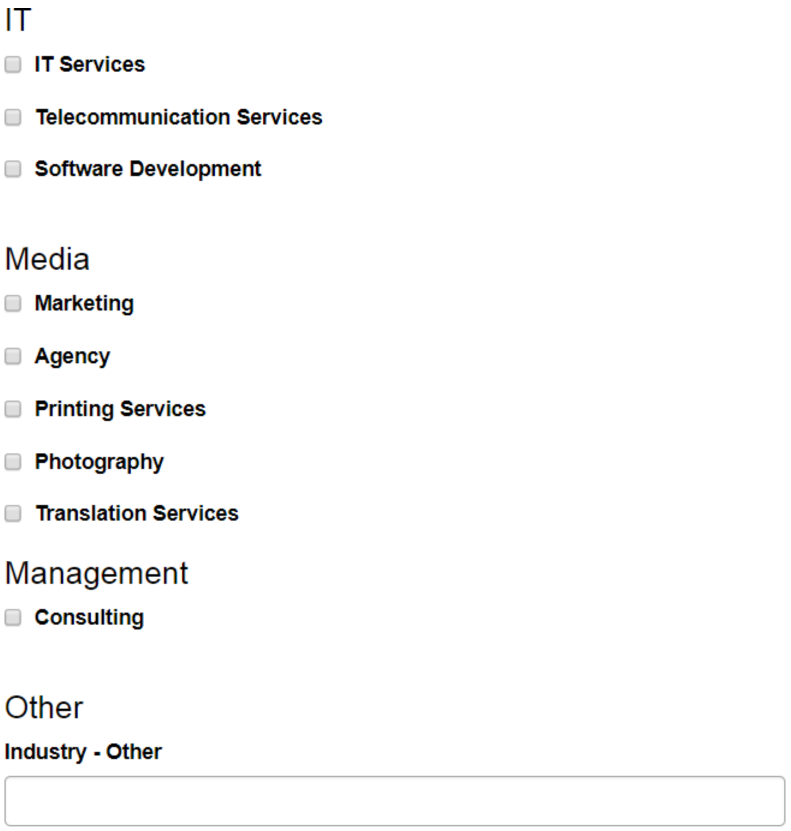
□ **Import, NSC**

□ **Dealership**

□ **Financial Services**

□ **Insurance**

□ **Claims Settlement**



IT

□ IT Services

□ Telecommunication Services

□ Software Development

Media

□ Marketing

□ Agency

□ Printing Services

□ Photography

□ Translation Services

Management

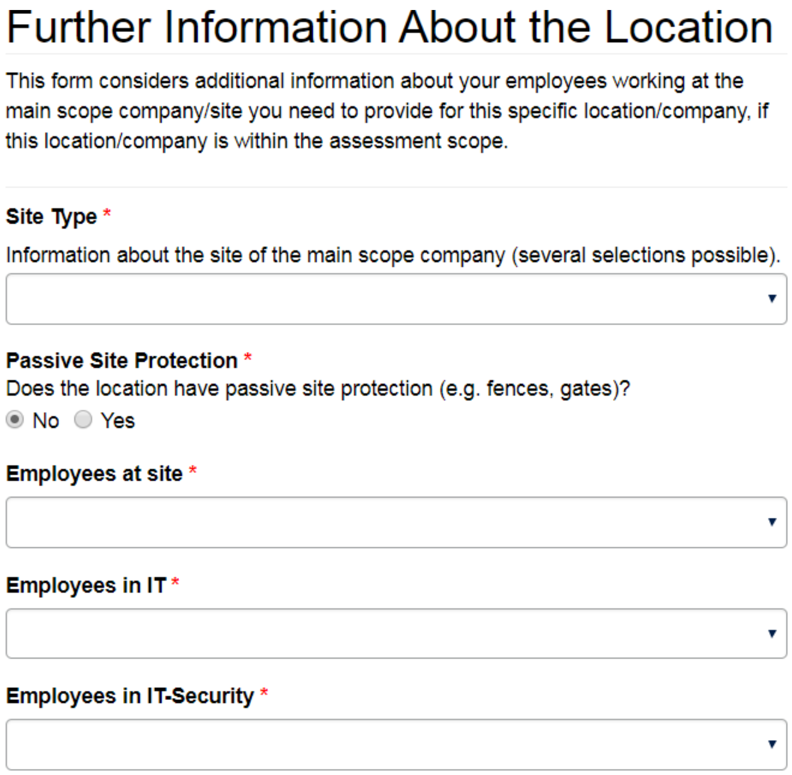
□ Consulting

Other

Industry - Other

Please note:

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”.



Further Information About the Location

This form considers additional information about your employees working at the main scope company/site you need to provide for this specific location/company, if this location/company is within the assessment scope.

Site Type *

Information about the site of the main scope company (several selections possible).

▾

Passive Site Protection *

Does the location have passive site protection (e.g. fences, gates)?

● No ○ Yes

Employees at site *

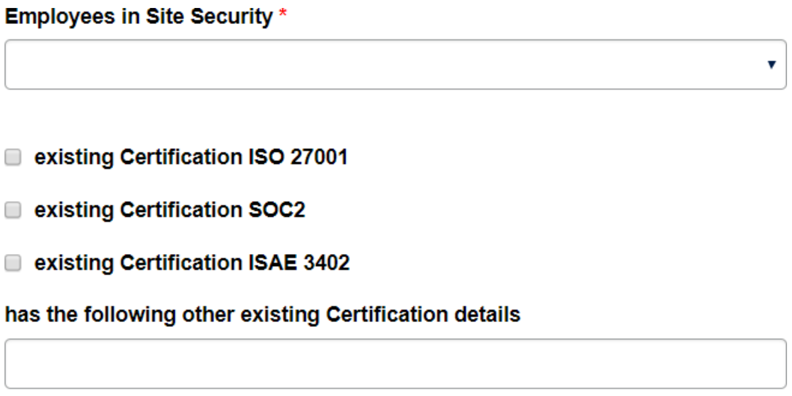
▾

Employees in IT *

▾

Employees in IT-Security *

▾



Employees in Site Security *

□ existing Certification ISO 27001

□ existing Certification SOC2

□ existing Certification ISAE 3402

has the following other existing Certification details

Figure 7: Details of every scope location

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 locations names based on the following pattern:

Pattern: [Geographical reference]

Example: for the fictitious company “ACME”

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

4.3.2.7 Scope name

For each scope you have to specify a “scope name”. The purpose of the scope name is to make it easier to refer to the scope in every TISAX-related communication (e.g. with your TISAX audit provider).

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 fictitious company “ACME”

- 2019
  (without geographical reference if your company has just one location)
- Frankfurt 2019
  (for a scope with several locations in the German **city** Frankfurt)
- *Lower Saxony 2019*
  (for a scope with all locations in the German **state** of Lower Saxony)
- Germany 2019
  (for a scope with all locations in the **country** Germany)
- EMEA 2019
  (for a scope with all locations in the **region** EMEA (“Europe, Middle East, Asia”))
- Prototype development 2019
  (*functional* reference for a scope with all locations involved in developing prototypes)

4.3.2.8 Contacts

For our communication with you, we collect information about contacts in 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 in your company will be a contact.

We ask for the following contact details (the red asterisk * indicates mandatory information in the online process):

Contact detail	Mandatory?	Example
Salutation	Yes	Mrs., Mr.
Academic degree		Dr., Ph.D., other
First name	Yes	John
Family name	Yes	Doe
Job Title	Yes	Head of IT
Role	Yes	CIO, ISMS manager, other
Department	Yes	Information Technology
Phone number	Yes	+49 69 986692777
Mobile number		
Email address	Yes	john.doe@acme.com
Country	Yes	Germany
Preferred language		English (default)
Other languages		German, French
Additional address information		Baloo Plaza, 2nd floor
Address identifier		HPC 1234
Street and number	Yes	Bockenheimer Landstraße 97-99
Postal code	Yes	60325
City	Yes	Frankfurt
Country	Yes	Germany

Table 1: Contact details

⚠ Important note:

We recommend assigning at least one deputy for each contact. If a contact is temporarily unavailable or leaves the company, there's someone else who 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 are legally allowed to speak for the company can approve of assigning a new main contact.

4.3.2.9 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 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[11].

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.[12]

   But if your partner is a large OEM, sometimes departments communicate the requirement to get TISAX-assessed, while not knowing their own company's Participant ID. In such cases you can contact us. We can provide you the Participant ID of your partner.
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 have to decide up to which level you want to grant access to your assessment result for your partner.

   For more information on sharing levels, please refer to section “6.5 Sharing levels” on page 82.

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 any publication or sharing.

For details please refer to section “6.4 Permanence of exchanged results” on page 82.

[11] 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.

[12] If you want to be on that list, please contact us.

For more information on publishing and sharing your assessment result, please refer to section “6 Exchange (Step 3)” on page 81.

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”) on page 33.

4.3.3.1 List of assessment objectives

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

You can 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.	Information with high protection needs	Info high
2.	Information with very high protection needs	Info very high
3.	Connection to 3rd parties with high protection needs	Con high
4.	Connection to 3rd parties with very high protection needs	Con very high
5.	Data protection According to article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	Data
6.	Data protection with special 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)	Special data
7.	Protection of prototype parts and components	Proto parts
8.	Protection of prototype vehicles	Proto vehicles
9.	Handling of test vehicles	Test vehicles
10.	Protection of prototypes during events and film or photo shootings	Events + Shootings

Table 2: The current TISAX assessment objectives

Example: If you are conducting test drives on public roads, then the assessment objective No. 9 “Handling of test vehicles” is one of your assessment objectives.

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

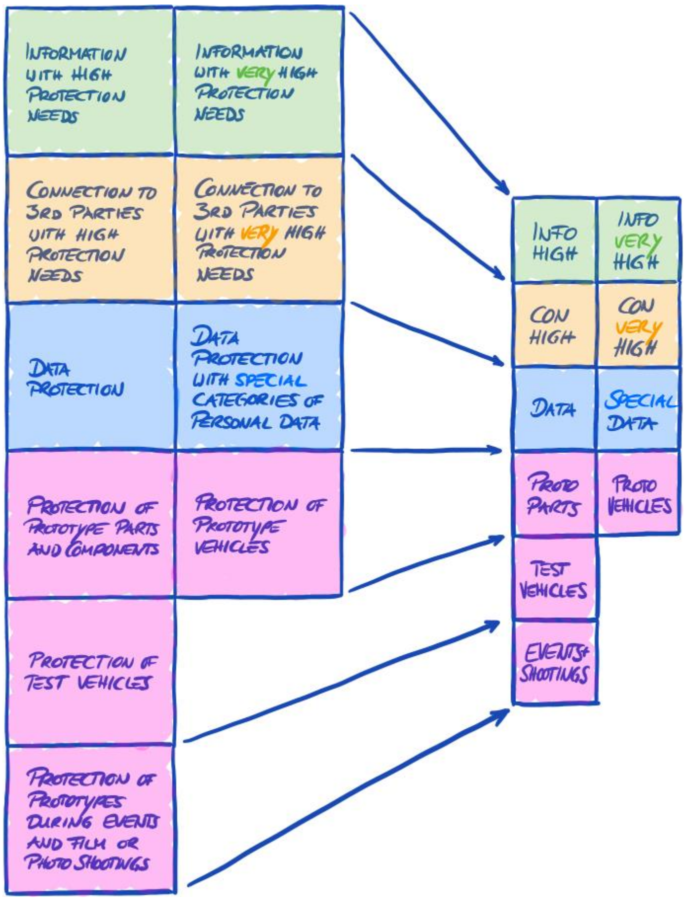

INFORMATION WITH HIGH PROTECTION NEEDS
INFORMATION WITH VERY HIGH PROTECTION NEEDS
CONNECTION TO 3RD PARTIES WITH HIGH PROTECTION NEEDS
CONNECTION TO 3RD PARTIES WITH VERY HIGH PROTECTION NEEDS
DATA PROTECTION
DATA PROTECTION WITH SPECIAL CATEGORIES OF PERSONAL DATA
PROTECTION OF PROTOTYPE PARTS AND COMPONENTS
PROTECTION OF PROTOTYPE VEHICLES
PROTECTION OF TEST VEHICLES
PROTECTION OF PROTOTYPES DURING EVENTS AND FILM OR PHOTO SHOOTINGS
INFO HIGH
INFO VERY HIGH
CON HIGH
CON VERY HIGH
DATA
SPECIAL DATA
PROTO PARTS
PROTO VEHICLES
TEST VEHICLES
EVENTS+ SHOOTINGS

Figure 8: 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” on page 33.

4.3.3.2 Assessment objectives and VDA ISA

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

Example: Both “Information” assessment objectives with high or very high protection needs map to the criteria catalogue “Information Security” of the VDA ISA. The Excel sheet is the same for both assessment objectives. You can distinguish the protection needs (high, very high) on the basis of the description of each requirement (under the respective subheading “Additionally in case of (very) high protection needs:”; see section “5.2.2 Understand the VDA ISA document” on page 48).

For further background information on the TISAX assessment objectives regarding their relationship to the VDA ISA criteria catalogues and the assessment levels, please refer to section “5.2.2 Understand the VDA ISA document” on page 48.

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 “Information with high protection needs”. Then you select “Information with high protection needs” as your assessment objective.

Figure 9 shows you the input and output of the TISAX process:

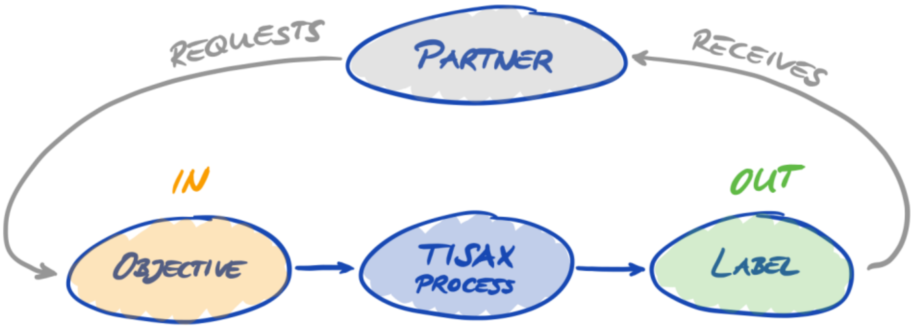


Figure 9: Assessment objectives and TISAX labels

For more information on TISAX labels, please refer to section “5.4.13 TISAX labels” on page 78.

4.3.3.4 Assessment objectives and their dependencies

The assessment objective “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 “Information with high protection needs” or “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”, then you automatically have to also achieve the assessment objective “Information with high protection needs”. You will find more information about the dependencies further down.

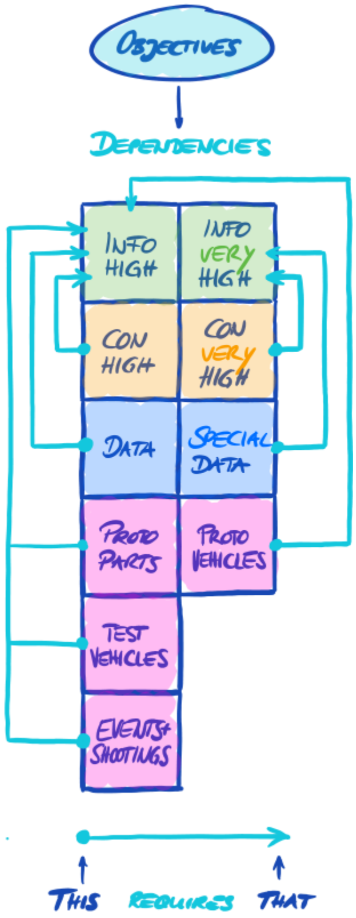


Figure 10: The assessment objectives and their dependencies

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:

a) you want to get TISAX-assessed before a partner asks for it, or

b) 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.	Information with high protection needs (Info high)	You may derive the protection needs (high, very high) from the document classification of your partner.
2.	Information with very high protection needs (Info very high)	
3.	Connection to 3rd parties with high protection needs (Con high)	Generally, this assessment objective applies when you have your own location (such as an office) on your partner's premises and you access your partner's applications via direct network connections. The use of this criteria catalogue among the OEMs is subject to individual interpretation. We therefore can't provide more advice here.
4.	Connection to 3rd parties with very high protection needs (Con very high)	
5.	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".
6.	Data protection with special categories of personal data (Special 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 special categories of personal data".
7.	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.
8.	Protection of prototype vehicles (Proto vehicles)	For all companies that manufacture, store 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 also receive the TISAX label "Protection of prototype parts and components".
9.	Handling of test vehicles (Test vehicles)	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. 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. 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".

10.	Protection of prototypes during events and film or photo shootings (Events + Shootings)	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. 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. 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”.

Table 3: Advice for the assessment objective selection

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 VDA 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 16: Requirements applicability to protection needs (example based on question 9.5) on page 52.

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 VDA 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 a VDA ISA criteria catalogue with either protection needs “high” or protection needs “very high”.

No.	VDA ISA criteria catalogue	Protection needs	TISAX assessment objective
1.	Information security	high	Information with high protection needs
2.	Information security	very high	Information with very high protection needs
3.	Connection to 3rd parties	high	Connection to 3rd parties with high protection needs
4.	Connection to 3rd parties	very high	Connection to 3rd parties with very high protection needs
5.	Data protection	high	Data protection According to article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)
6.	Data protection	very high	Data protection with special 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)
7.	Prototype protection	high	Protection of prototype parts and components

8.	Prototype protection	high	Protection of prototype vehicles
9.	Prototype protection	high	Handling of test vehicles
10.	Prototype protection	high	Protection of prototypes during events and film or photo shootings

Table 4: Mapping of VDA 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 his information. Therefore, TISAX differentiates three “assessment levels” (AL). The assessment level defines the depth to which our TISAX audit providers have to look and which audit methods they have to apply. Simplified, this means a higher assessment level results in a higher assessment intensity and the use of more enhanced assessment methods.

No.	TISAX assessment objective	Assessment level (AL)
1.	Information with high protection needs	AL 2
2.	Information with very high protection needs	AL 3
3.	Connection to 3rd parties with high protection needs	AL 2
4.	Connection to 3rd parties with very high protection needs	AL 3
5.	Data protection According to article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	AL 2
6.	Data protection with special 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 3
7.	Protection of prototype parts and components	AL 3
8.	Protection of prototype vehicles	AL 3
9.	Handling of test vehicles	AL 3
10.	Protection of prototypes during events and film or photo shootings	AL 3

Table 5: Mapping of the TISAX assessment objectives to assessment levels

Assessment level 1 (AL 1):

Assessments with assessment level 1 mostly play a role for internal purposes in the true sense of a self-assessment.

For an assessment with 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 evidences.

Results of assessments with 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 with assessment level 2, the audit provider does a plausibility check on your self-assessment (for all locations within assessment scope). He supports this by checking evidences[13] and conducting interviews with you and further colleagues.

The audit provider does the interviews generally by audio conference. Upon your request, he can conduct the interviews in person.

Assessments with assessment level 2 generally do not include an on-site inspection. However, assessments always include an on-site inspection, if one of the following conditions is true:

- You have the assessment objective “Handling of prototypes” (regardless of the protection needs).
- You have the assessment objective “Connection to 3rd parties”[14] (regardless of the protection needs).
- Your location is in a country that is listed in the “TISAX activation list”.
  You don't need to refer to the “TISAX activation list” if your location is in a country that is member of the EU[15] or the G7[16]. For all other countries, please download the “TISAX activation list” at:

  🇬🇧 https://www.enx.com/tisax/files/downloads/ACAR/TISAX - Activation List(621).pdf

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

Assessment level 3 (AL 3):

For an assessment with assessment level 3, the audit provider does all the checks as for an assessment with assessment level 2. However, all checks will be more comprehensive, and he will thoroughly verify your self-assessment result in an in-depth on-site inspection and interviews in person.

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
Evidences	No	Plausibility check	Thorough verification
Interviews	No	By audio conference[17]	In person, on site
On-site inspection	No	In certain cases[18]	Yes

Table 6: Applicability of assessment methods to different assessment levels

[13] Evidences are anything that supports your assertion that you fulfil a certain requirement. Evidences are mostly documents. You will surely use internal documentation as evidence.

[14] These two assessment objectives focus in large parts on physical security. Therefore, an on-site inspection is mandatory to verify the fulfilment of the physical security requirements.

[15] https://en.wikipedia.org/wiki/Member_state_of_the_European_Union#List

[16] https://en.wikipedia.org/wiki/Group_of_Seven

[17] Interviews for assessments with assessment level 2 are generally conducted by audio conference. Upon your request, interviews can be conducted on site. Furthermore, interviews for assessments of locations in countries that are listed in the “TISAX activation list” are always held on site, even for assessments with assessment level 2.

[18] Assessments of locations in countries that are listed in the “TISAX activation list” always include an on-site inspection.

Additional information:

- Information classification and protection needs

  The mapping of information classification (like confidential, 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 mapping table where the information classification of your partner precisely 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 a VDA 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 can 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 to select assessment objectives that imply an assessment level 3. The efforts for TISAX assessments with assessment level 3 are not generally higher than those with assessment level 2.

  Especially those 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 with assessment level 2 is lower, your internal efforts may be higher. This is due to the fact that for an assessment with assessment level 2 usually requires a more comprehensive self-assessment and a better internal documentation. For assessments with assessment level 3, showing things together with some basic documentation is often enough evidence for the auditor. But without an on-site inspection, the auditor will request precise documentation. Thus, choosing assessment level 3 over assessment level 2 is not uncommon. Yet it is a choice rather made by smaller than larger companies.

4.3.4 Fee

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

You can download the price list on our website at:

https://enx.com/tisax/tisax-en.html#registration (“TISAX Price List” in the column on the right)

Direct PDF download:

https://www.enx.com/tisax/files/downloads/TISAX-Price-List-current.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.

Please consider thoroughly checking the invoice address. Accounting laws require that the address on our invoice exactly matches your company's (invoice) address.

- Changing the invoice address

  In contrast to all other information you provide, we can't change the invoice address once you have selected it in the process. Please contact us if you need to receive the invoice at another address.

  Please note: Should you pause and resume the registration process before you have selected an invoice address, you won't be able to do this later. We will notice missing invoice addresses, contact you in order to obtain this information and add it for you.

- 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) as far as 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 (no credit card payments).
- 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 at section “7.1 Annexe: Example invoice” on page 86.
- 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 an up-to-date version.

ℹ 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 ultimately 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” on page 65.

⚠ 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 went 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).

4.5 Online registration process

If you prepared yourself according to our advice above (“4.3 Registration preparation” on page 16), 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 a registration as 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 need to interrupt nevertheless, we will contact you to request any missing data.

4.5.2 Start here

Please start your registration on our website at:

🇬🇧 https://enx.com/tisax/tisax-en.html#registration

Basically, you just need to follow the on-screen instructions. Nevertheless, we briefly describe the sequence below.

4.5.3 Portal account

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

By creating this account, you don't automatically become an official TISAX contact inside your company[19]. Right now, you just fill out our online forms. You can define the "participant contact" and "scope contact" later in the online registration process and assign these roles to others.

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 other 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), please contact us. We will send an invitation email to the contact. The email contains a link that will lead to the creation of a portal account for the contact.

Please ensure you have already created the new contact before asking us to assign this right.

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

We request you to specify the main 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 primary 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, you can add additional participant contacts.

Important note:

We recommend assigning at least one deputy for each contact. If a contact is temporarily unavailable or leaves the company, there's someone else who 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

[19] Our regular communication by email is only sent to participant contacts. It is not sent to accounts that do not have the participant role. To have our emails sent to account owners as well, please ensure that they also defined at least as additional participant contact.

complex process. Our process ensures that only persons who are legally allowed to speak for the company can approve of 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).

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” on page 17.

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.

  We will use the “scope name” to reference to this scope in further communication.
- 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” on page 18.
- specify the main scope contact.

  This is the person that 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 and our TISAX audit providers 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” on page 27.
- add assessment scope location(s).

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

  You may want to refer back to the explanatory notes in “4.3.2 The TISAX assessment scope” on page 18.

  Please note:

  You can always add or remove locations at a later point in time (even after completing the online registration process; but only before you completed the assessment whereof a location is part of).
- 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 at least allow us to 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 the access to your assessment result later.

  You may want to refer back to the explanatory notes in “4.3.2.9 Publication and sharing” on page 26.

Important note:

You can't revoke any publication or sharing permissions.

For details please refer to section "6.4 Permanence of exchanged results" on page 82.

- specify who receives the invoice.

  You are requested to specify who will receive our invoice(s).

  You may want to refer back to the explanatory notes in section "4.3.4 Fee" on page 36.

Please note:

Every assessment scope runs through a life cycle. At this stage, your assessment scope either has the status "Incomplete" or "Awaiting approval".

For more information on the status of an assessment scope, please refer to section "7.5.1Assessment scope status overview" on page 91.

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[20] and
- your information security management system is in top form and centrally organised[21].

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:

🇬🇧 https://enx.com/tisax/tisax-en.html#registration ("TISAX Simplified Group Assessment" in the column on the right)

Direct PDF download:

🇬🇧 https://enx.com/tisax/files/downloads/TISAX-Simplified-Group-Assessment-current.pdf

Please note:

Currently it is not possible to delete an assessment scope in the ENX portal. In case 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.

[20] The theoretical minimum for simplified group assessments is three locations.

[21] If you already know you will have to improve your information security management system, the recommended minimum is at least twelve locations.

For more information on audit provider selection, please refer to section “5.3 Audit provider selection” on page 64.

- 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 Annexe: Example confirmation email” on page 87.

For an example of the “TISAX Scope Excerpt”, please refer to section “7.3 Annexe: Example TISAX Scope Excerpt” on page 88.

You will receive our confirmation email usually within 3 business days.

If you don't hear from us within 7 business days, please verify that you provided all information. We only start processing your registration when everything is complete. If you think everything is complete yet we haven't contacted you, then please get in touch with us.

We send our confirmation email to the main participant contact and to all additional participant contacts.

Please note:

Every assessment scope runs through a life cycle. At this stage, your assessment scope has the status “Approved”.

For more information on the status of an assessment scope, please refer to section “7.5.4 Assessment scope status “Approved” on page 94.

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:

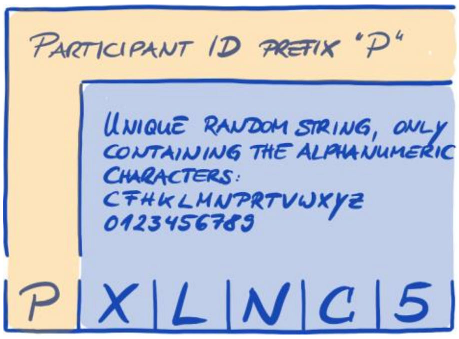

PARTICIPANT ID PREFIX "P"
UNIQUE RANDOM STRING, ONLY CONTAINING THE ALPHANUMERIC CHARACTERS:
CFHKLMNPRTVWXYZ
0123456789
P
X
L
N
C
5

Figure 11: Format of the Participant ID[22]

Please note:

There are two ways to find your Participant ID:

1. Check your “TISAX Scope Excerpt”.

   Please refer to the section “Confirmation email” above.

   If you don't have your “TISAX Scope Excerpt” at hand, please contact us to obtain it.
2. Log in to the ENX portal, go to the main navigation bar, select “MY ENX PORTAL” and then “MY SCOPES AND ASSESSMENTS”. 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:

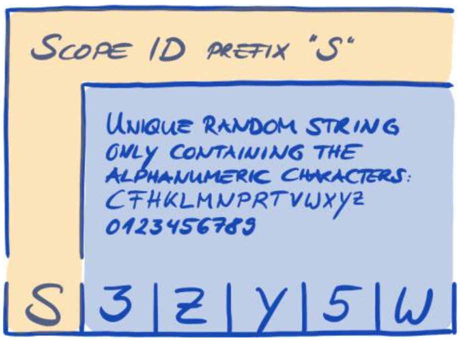

SCOPE ID PREFIX "S"
UNIQUE RANDOM STRING ONLY CONTAINING THE ALPHANUMERIC CHARACTERS:
CFHKLMNPRTVWXYZ
0123456789
S
3
Z
Y
5
W

Figure 12: Format of the Scope ID

[22] 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”.

Please note:

There are two ways to find your Scope ID:

1. Check your “TISAX Scope Excerpt”.

   Please refer to the section “Confirmation email” above.

   If you don't have your “TISAX Scope Excerpt” at hand, please contact us to obtain it.

2. Log in to the ENX portal, go to the main navigation bar, select “MY ENX PORTAL” and then “MY 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 Annexe: Assessment scope status” on page 91.

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:

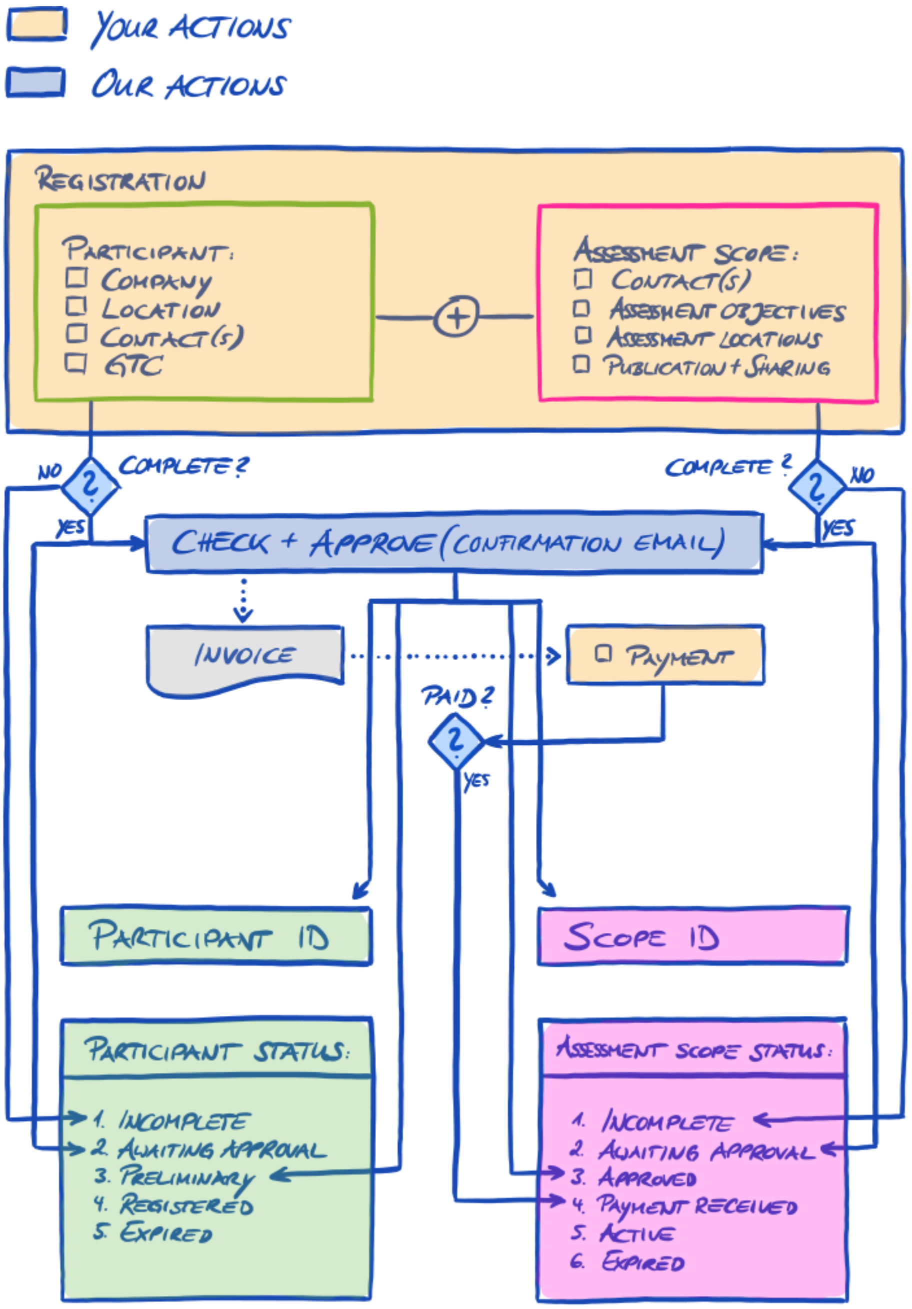


Figure 13: Conditions for the participant status and assessment scope status

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

For more information on the:

- participant status, please refer to section “7.4 Annexe: Participant status” on page 90.
- assessment scope status, please refer to section “7.5 Annexe: Assessment scope status” on page 93.

4.5.10 Changes of your registration information

Please note:

For all answers regarding the data life cycle, please refer to section “7.7 Annexe: Participant data life cycle management” on page 97. 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 VDA 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 VDA 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 VDA ISA.

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

The explanations, examples and screenshots in this handbook are based on “Version: 4.1.0 / 2018-12-13” of the VDA ISA document.

Please note:

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

You can find further hints in the Excel sheets of each criteria catalogue in column G/Version. It indicates in which version the VDA added/changed a requirement.

Important note:

While the VDA ISA is based on the standard ISO/IEC 27001, you don't have to be certified according to it in order to pass a TISAX assessment.

5.2.1 Download the VDA ISA document

Start your self-assessment with downloading the VDA ISA document.

You can download it at the VDA website:

https://www.vda.de/en/topics/safety-and-standards/information-security/information-security-requirements

Direct download (Excel spreadsheet):

https://www.vda.de/dam/vda/Medien/DE/Themen/Sicherheit-und-Standards/Informationssicherheit/VDA-ISA_EN_4-1-0.xlsx

The VDA ISA is also available in German:

https://www.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen

Direct download (Excel spreadsheet):

https://www.vda.de/dam/vda/Medien/DE/Themen/Sicherheit-und-Standards/Informationssicherheit/VDA-ISA_DE_4-1-0.xlsx

5.2.2 Understand the VDA 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 VDA ISA document, but with a focus on the use for TISAX assessments.

5.2.2.1 Criteria catalogues

The VDA ISA currently contains four "criteria catalogues"[23]:

1.	Information security
2.	Connection to 3rd parties
3.	Data protection
4.	Prototype protection

Each criteria catalogue has its own Excel sheet:

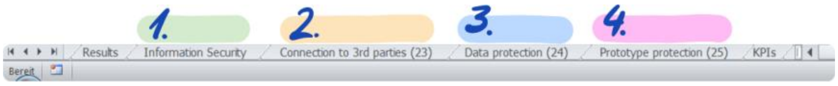


Figure 14: Screenshot: VDA ISA criteria catalogues as Excel sheets

The core of the VDA 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	VDA ISA criteria catalogue
1.	Information with high protection needs	Information security
2.	Information with very high protection needs	Information security
3.	Connection to 3rd parties with high protection needs	Connection to 3rd parties

[23] The VDA ISA also refers to the criteria catalogues as "modules".

4.	Connection to 3rd parties with very high protection needs	Connection to 3rd parties
5.	Data protection According to article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	Data protection
6.	Data protection with special 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
7.	Protection of prototype parts and components	Prototype protection
8.	Protection of prototype vehicles	Prototype protection
9.	Handling of test vehicles	Prototype protection
10.	Protection of prototypes during events and film or photo shootings	Prototype protection

Table 7: Mapping between TISAX assessment objectives and VDA ISA criteria catalogues

Example: If you have selected the assessment objective “Data protection”, then you will have to answer the questions in the criteria catalogue “Information security” AND in the criteria catalogue “Data protection”.

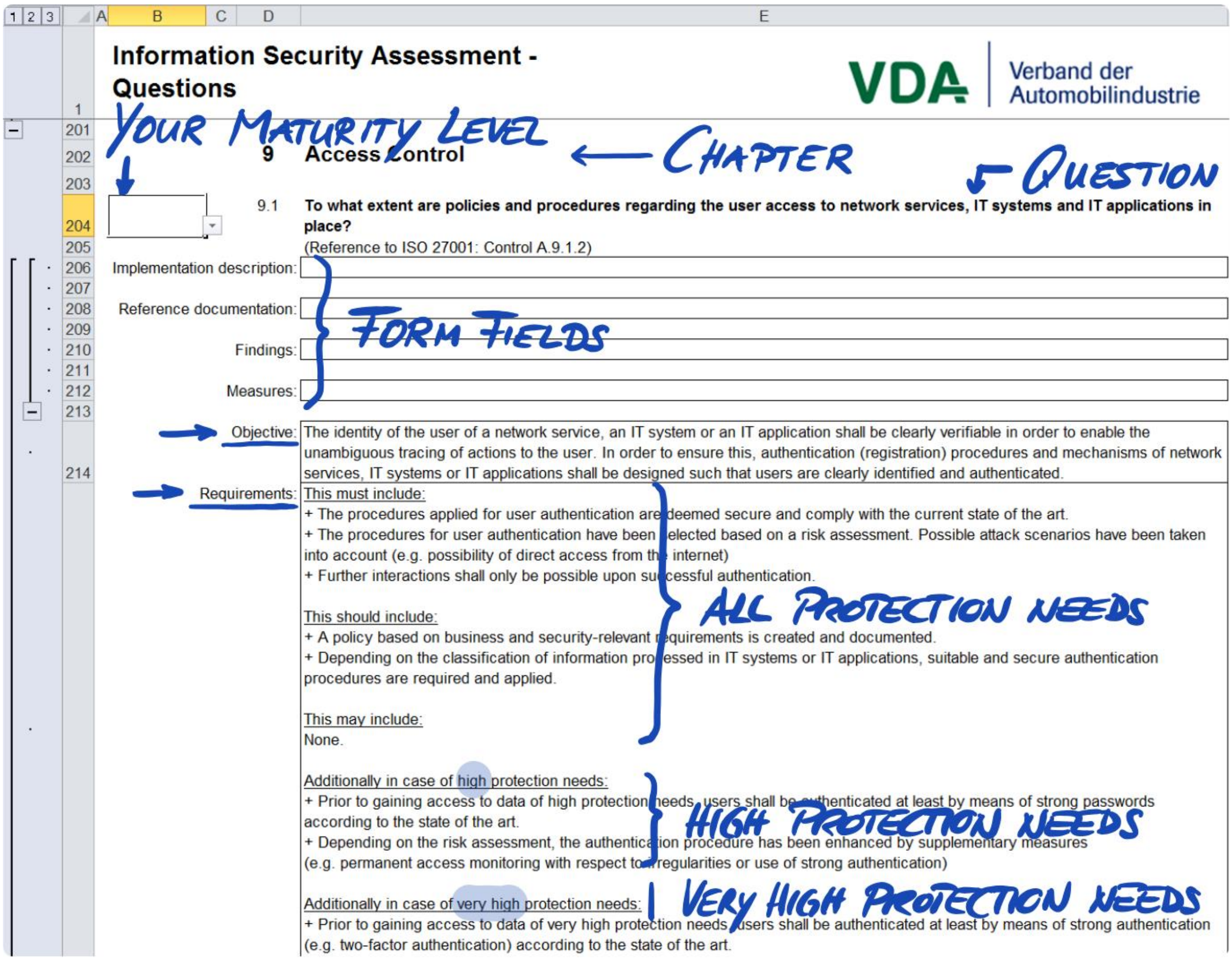
You may have noticed that there is more than one assessment objective per criteria catalogue. How do you know which requirements are applicable to which assessment objective? For the first three criteria catalogues, the difference lies in the protection needs. For more information, please refer to section “5.2.2.6 Requirements” on page 52.

For the fourth criteria catalogue (“Prototype protection”), a subset of the five chapters is applicable for each assessment objective:

No.	Assessment objective	Applicable chapters
7.	Protection of prototype parts and components	25.1 Physical and Environmental Security 25.2 Organizational Requirements 25.3 Handling of vehicles, components and parts
8.	Protection of prototype vehicles	25.1 Physical and Environmental Security 25.2 Organizational Requirements 25.3 Handling of vehicles, components and parts (plus the additional requirements for handling vehicles with protection needs, as mentioned in the requirements section of each question (if applicable))
9.	Handling of test vehicles	25.2 Organizational Requirements 25.3 Handling of vehicles, components and parts 25.4 Requirements for test vehicles
10.	Protection of prototypes during events and film or photo shootings	25.2 Organizational Requirements 25.3 Handling of vehicles, components and parts 25.5 Requirements for events and photo/film productions

Table 8: The applicable chapters of the criteria catalogue “Prototype protection” for the respective assessment objectives

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



Information Security Assessment - Questions

9 Access Control

9.1 **To what extent are policies and procedures regarding the user access to network services, IT systems and IT applications in place?**
(Reference to ISO 27001: Control A.9.1.2)

Implementation description:

Reference documentation:

Findings:

Measures:

Objective: The identity of the user of a network service, an IT system or an IT application shall be clearly verifiable in order to enable the unambiguous tracing of actions to the user. In order to ensure this, authentication (registration) procedures and mechanisms of network services, IT systems or IT applications shall be designed such that users are clearly identified and authenticated.

Requirements: This must include:
+ The procedures applied for user authentication are deemed secure and comply with the current state of the art.
+ The procedures for user authentication have been selected based on a risk assessment. Possible attack scenarios have been taken into account (e.g. possibility of direct access from the internet)
+ Further interactions shall only be possible upon successful authentication.

This should include:
+ A policy based on business and security-relevant requirements is created and documented.
+ Depending on the classification of information processed in IT systems or IT applications, suitable and secure authentication procedures are required and applied.

This may include:
None.

Additionally in case of high protection needs:
+ Prior to gaining access to data of high protection needs, users shall be authenticated at least by means of strong passwords according to the state of the art.
+ Depending on the risk assessment, the authentication procedure has been enhanced by supplementary measures (e.g. permanent access monitoring with respect to irregularities or use of strong authentication)

Additionally in case of very high protection needs:
+ Prior to gaining access to data of very high protection needs, users shall be authenticated at least by means of strong authentication (e.g. two-factor authentication) according to the state of the art.

Figure 15: Screenshot: Main elements of the questions in the VDA ISA criteria catalogues

5.2.2.2 Chapters

Each criteria catalogue groups the questions in chapters.

Example: “9 Access Control”

The grouping is based on the various aspects of information security management systems.

5.2.2.3 Questions

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

Example: “9.1 To what extent are policies and procedures regarding the access to IT systems in place?”[24]

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

[24] The numbering scheme for the questions is based on the control numbers in ISO/IEC 27001. This also explains gaps in the numbering sequence (example: questions 2-4 are “missing”).

5.2.2.4 Self-assessment form fields

Below the questions are form fields you need to fill when you are conducting a self-assessment:

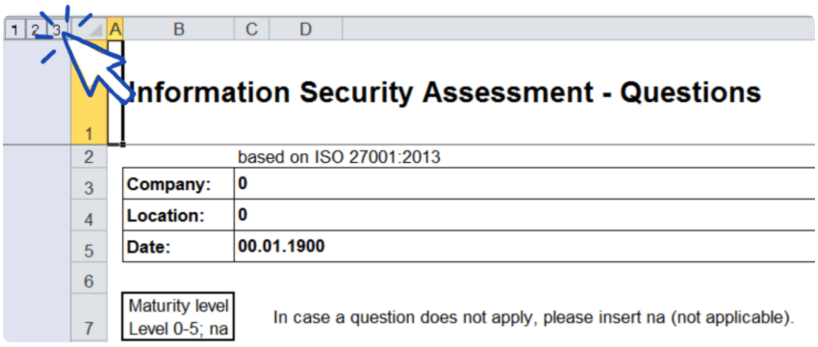
Form field	Purpose	Mandatory?
Implementation description	Here you should briefly describe what you implemented to address this question in your company.	Yes
Reference documentation	Here you should specify in which document(s) you prove the implementation.	Yes
Findings	Here you can write down any findings where you think a gap exists between what should be and what is.	No
Measures	Here you can write down any tasks or measures you plan to complete to close any gaps and to improve your information security management system.	No

Table 9: 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.

Important note:

If you open the downloaded Excel file and select one of the criteria catalogue worksheets (like 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 “3”[25]. You find the button just a bit up and left from cell A1. This will expand the view to show the self-assessment form fields below each question.



Information Security Assessment - Questions

based on ISO 27001:2013

Company:	0
Location:	0
Date:	00.01.1900

Maturity level Level 0-5; na

In case a question does not apply, please insert na (not applicable).

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 very good fine motor skills. Using your pointing device's scroll feature, you may also involuntarily “skip” over some of the larger cells.

Alternatively, you can click on the grouping button for level “1”. This will show you just the questions.

A click on the grouping button for level “2” will again show the default view.

5.2.2.5 Objective

Behind every question is an objective. It describes what you need to achieve regarding this aspect of your information security management.

Example (for question 9.1): “The identity of the user of a network service, an IT system or an IT application must be clearly verifiable to enable to a trace of actions unambiguously to the user. In order to ensure this, authentication

[25] You can find the underlying Excel feature in the ribbon “Data” (German: “Daten”), section “Outline” (German: Gliederung).

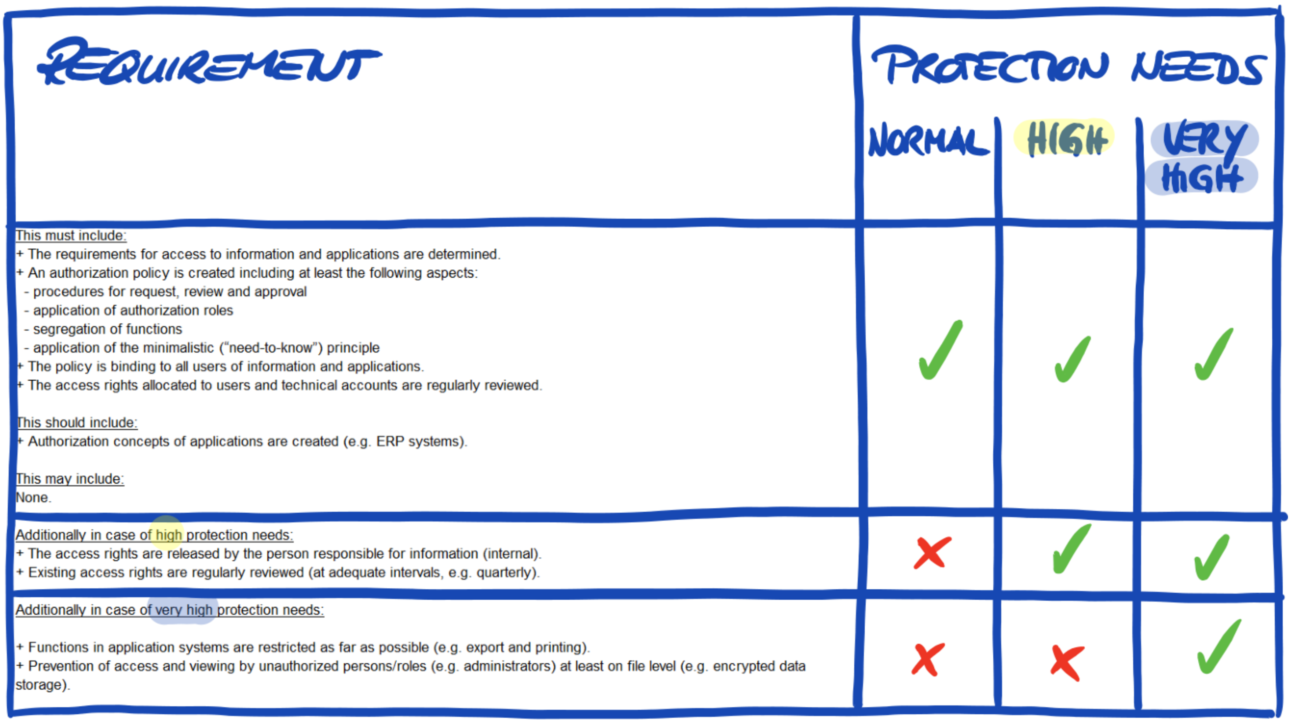
(registration) procedures and mechanisms of IT systems or IT applications must be designed such that users are clearly identified and authenticated.”

5.2.2.6 Requirements

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

There may be additional requirements for higher protection needs. You have to fulfil all requirements up to the protection need you need to achieve (which you can derive from your assessment objective).

Figure 17 illustrates the applicability of requirements to a certain protection need:



REQUIREMENT	PROTECTION NEEDS		
	NORMAL	HIGH	VERY HIGH
This must include: + The requirements for access to information and applications are determined. + An authorization policy is created including at least the following aspects: - procedures for request, review and approval - application of authorization roles - segregation of functions - application of the minimalistic ("need-to-know") principle + The policy is binding to all users of information and applications. + The access rights allocated to users and technical accounts are regularly reviewed. This should include: + Authorization concepts of applications are created (e.g. ERP systems). This may include: None.	✓	✓	✓
Additionally in case of high protection needs: + The access rights are released by the person responsible for information (internal). + Existing access rights are regularly reviewed (at adequate intervals, e.g. quarterly).	✗	✓	✓
Additionally in case of very high protection needs: + Functions in application systems are restricted as far as possible (e.g. export and printing). + Prevention of access and viewing by unauthorized persons/roles (e.g. administrators) at least on file level (e.g. encrypted data storage).	✗	✗	✓

Figure 16: Requirements applicability to protection needs (example based on question 9.5)

But for many questions, there are no additional requirements for higher protection needs.

Additionally, the VDA ISA categorises the requirements into these three requirements levels[26]:

Requirements level	Text	Explanation
Must	“This must include”	You must fulfil these requirements without exception.
Should	“This should include”	You should fulfil these requirements. There may be reasons why you don't fulfil a requirement. If you don't fulfil a requirement of this level, you must be able to show that you understand the implications and be able to explain and justify it.
May	“This may include”	You may fulfil these requirements. Requirements of this level show additional or alternative ways to achieve the objective.

Table 10: VDA ISA requirements levels and their explanations

The requirements that apply to all protection needs can be of any of the three levels described above. If there are additional requirements for high protection needs or very high protection needs, the requirements level is always “Must” (if not stated otherwise).

Question 9.5 is an example which has additional requirements for both protection needs “high” and “very high” (see figure 16).

Important note:

It is very important for you to understand that even fulfilling all the requirements does NOT automatically guarantee that the audit provider confirms that you achieve the objective.

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

The audit provider always has to 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.

In case of doubt, you can get consulting from our TISAX audit providers.

For more information, please refer to section “5.2.5 Address the self-assessment result” on page 63.

5.2.2.7 Maturity levels

The VDA 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 VDA 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 provide you our simplified one-sentence-summary for each level:

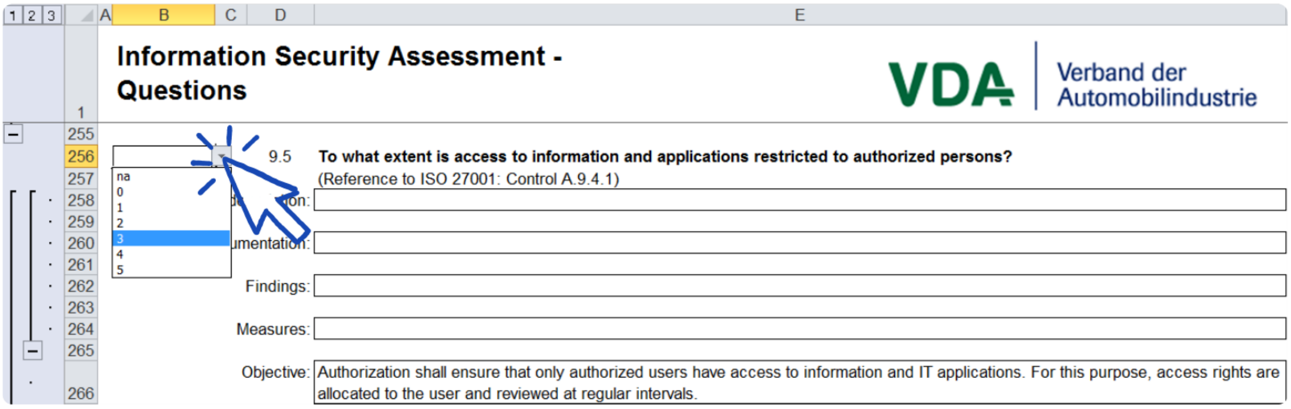
Maturity level	In one word	In one sentence
0	Incomplete	There is no process, or the process does not work.
1	Performed	There is a process and the result suggests it works, but the process is not documented and nobody knows for sure why the process works.
2	Managed	There are processes that work and are documented, but there are many different processes for the same objective.

[26] The VDA ISA interprets the key words “MUST”, “SHOULD” and “MAY” as described in “RFC 2119 Key words for use in RFCs to Indicate Requirement Levels”, https://www.ietf.org/rfc/rfc2119.txt.

3	Established	There is a process that works and has documentation that is up-to-date and maintained.
4	Predictable	Same as for level 3, plus the process is measured.
5	Optimizing	Same as for level 4, plus dedicated staff is responsible for continual improvements.

Table 11: Simplified one-sentence-summaries of the maturity levels

You have to rate the maturity level of your information security management system per question. Select your maturity level in the drop-down menu left to the question (Column B).



Information Security Assessment - Questions

9.5 To what extent is access to information and applications restricted to authorized persons?
(Reference to ISO 27001: Control A.9.4.1)

on:

umentation:

Findings:

Measures:

Objective: Authorization shall ensure that only authorized users have access to information and IT applications. For this purpose, access rights are allocated to the user and reviewed at regular intervals.

Figure 17: Screenshot: Example of maturity level selection in the VDA 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" on page 55.

5.2.2.8 Further explanations

The definitions of maturity level 2 and above (Excel sheet "Definitions") contain:

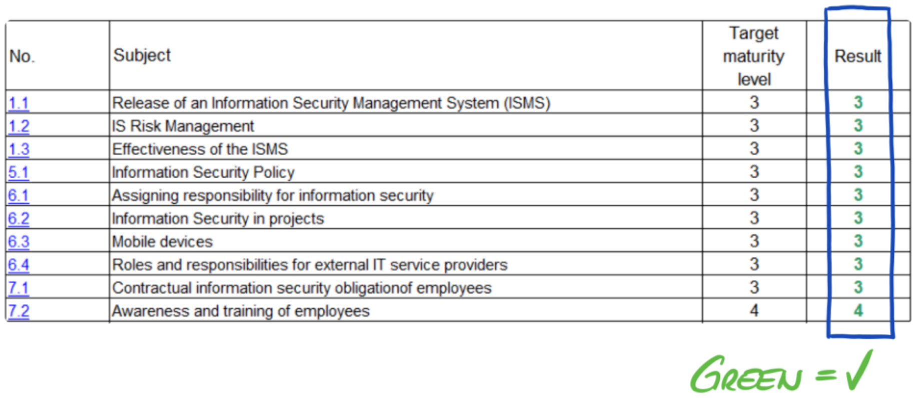
- the abbreviation "PA". It stands for "process attribute" and is defined in the glossary sheet of the Excel file. These attributes describe your process ("things your process does").
- the abbreviation "GWP". It stands for "generic work product" and is defined in the glossary sheet of the Excel file. These "products" are mainly documents. They are physical artefacts that belong to or stem from your process.

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 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" should be completely filled, either with numbers (0-5) or "na" (as in "not applicable").



No.	Subject	Target maturity level	Result
1.1	Release of an Information Security Management System (ISMS)	3	3
1.2	IS Risk Management	3	3
1.3	Effectiveness of the ISMS	3	3
5.1	Information Security Policy	3	3
6.1	Assigning responsibility for information security	3	3
6.2	Information Security in projects	3	3
6.3	Mobile devices	3	3
6.4	Roles and responsibilities for external IT service providers	3	3
7.1	Contractual information security obligationof employees	3	3
7.2	Awareness and training of employees	4	4

Figure 18: Screenshot: Example of "Results" sheet in the VDA ISA document (cell B16)

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

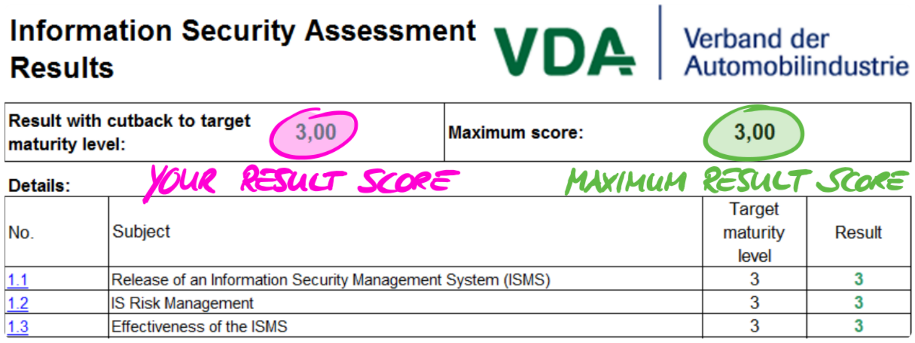
5.2.4 Interpret the self-assessment result

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

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" (cell D14). We will explain the "cutback" soon.



Information Security Assessment Results

VDA Verband der Automobilindustrie

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

Details:

No.	Subject	Target maturity level	Result
1.1	Release of an Information Security Management System (ISMS)	3	3
1.2	IS Risk Management	3	3
1.3	Effectiveness of the ISMS	3	3

Figure 19: Screenshot: Your result score and the maximum result score (Excel sheet "Results", cell D14 and G14)

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

1. Question level

   On this level, there are 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:

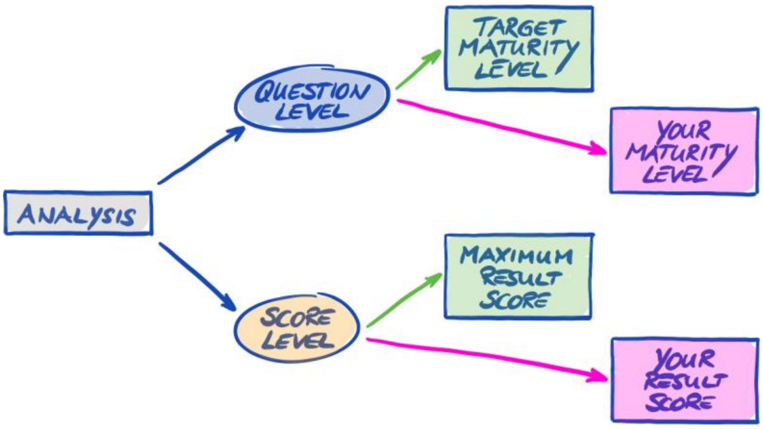
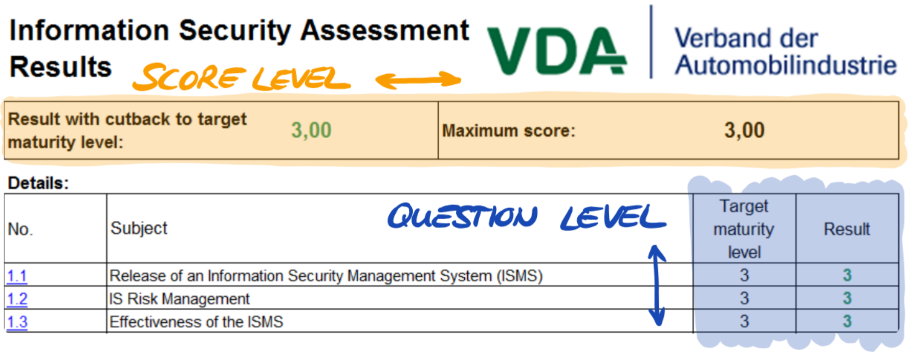


Figure 20: Analysis of the self-assessment result on the question level and the score level

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

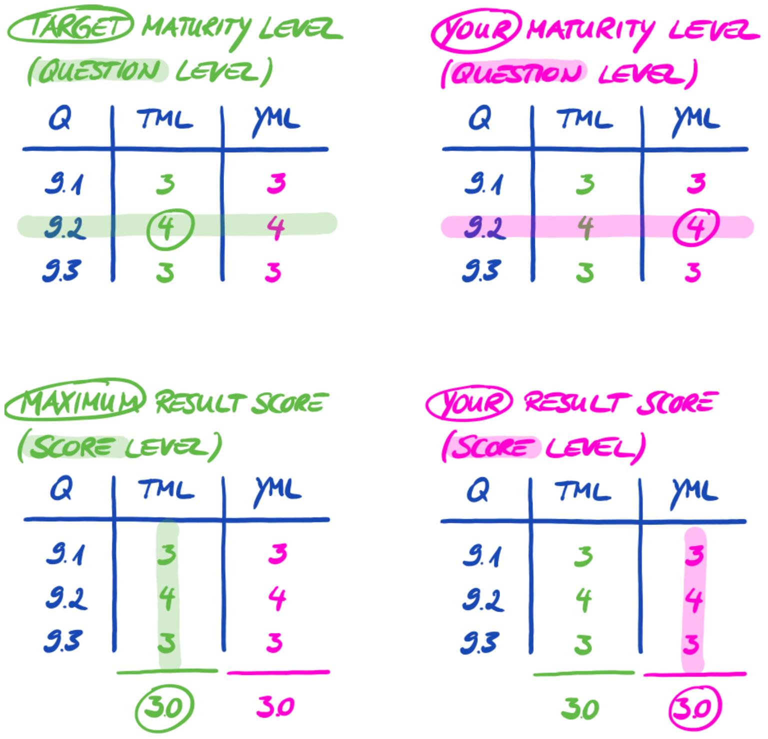
Result with cutback to target maturity level:	3,00	**Maximum score:**	3,00

Details:

No.	Subject	Target maturity level	Result
1.1	Release of an Information Security Management System (ISMS)	3	3
1.2	IS Risk Management	3	3
1.3	Effectiveness of the ISMS	3	3

Figure 21: Score level and question level in the Excel sheet "Results"

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



TARGET MATURITY LEVEL (QUESTION LEVEL)

Q	TML	YML
9.1	3	3
9.2	4	4
9.3	3	3

YOUR MATURITY LEVEL (QUESTION LEVEL)

Q	TML	YML
9.1	3	3
9.2	4	4
9.3	3	3

MAXIMUM RESULT SCORE (SCORE LEVEL)

Q	TML	YML
9.1	3	3
9.2	4	4
9.3	3	3
	3.0	3.0

YOUR RESULT SCORE (SCORE LEVEL)

Q	TML	YML
9.1	3	3
9.2	4	4
9.3	3	3
	3.0	3.0

Figure 22: The targets and your results on the question level and the score level

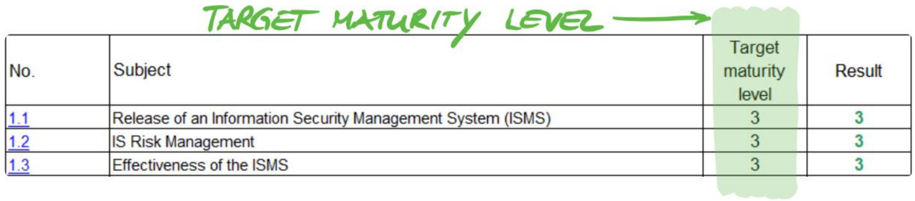
The following sections explain the result and its analysis in detail.

5.2.4.2 The target maturity level (on question level)

The VDA ISA defines a "target maturity level" for each question. The target maturity levels vary between 2 and 4, but most of them are 3. The average target maturity level for all questions combined is 3.

For more information on the definition of each maturity level, please refer to section "5.2.2 Understand the VDA ISA document" on page 48.

The VDA ISA defines the target maturity levels in the Excel sheet "Results" (starting at column G, row 17; see figure below).



No.	Subject	Target maturity level	Result
1.1	Release of an Information Security Management System (ISMS)	3	3
1.2	IS Risk Management	3	3
1.3	Effectiveness of the ISMS	3	3

Figure 23: The target maturity level definition in the Excel sheet "Results"

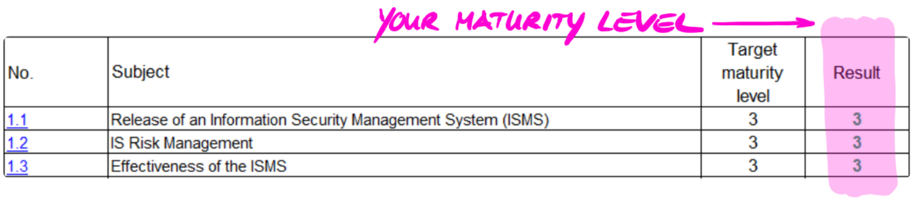
5.2.4.3 Your result (on question level)

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 per question. If the target maturity level for two questions is “3”, you can't compensate a maturity level of “2” in one question with a maturity level of “4” in the other question.

The VDA ISA document automatically transfers your maturity levels from the Excel sheet “Information security” (column B) to the Excel sheet “Results” (starting at column G, row 17):



No.	Subject	Target maturity level	Result
1.1	Release of an Information Security Management System (ISMS)	3	3
1.2	IS Risk Management	3	3
1.3	Effectiveness of the ISMS	3	3

Figure 24: Your maturity levels in the Excel sheet “Results”

Your maturity level is subject to a calculation before the VDA 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 questions where your maturity level is *below* the target maturity level.

Here's how the VDA 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”.

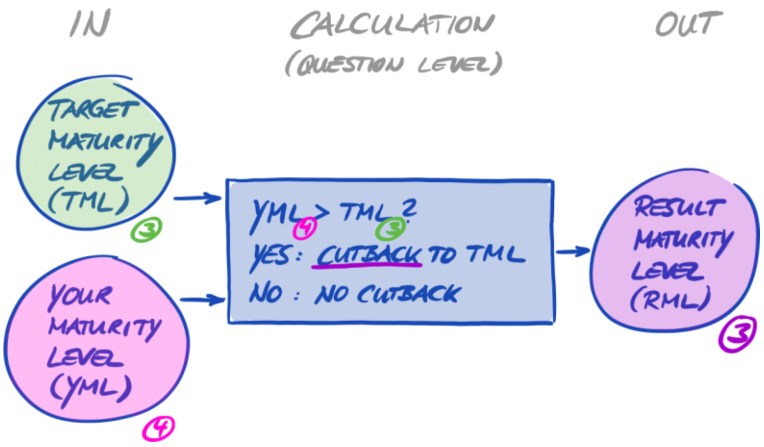


Figure 25: Cutback calculation of the result maturity level

The figure below shows that if your maturity level is higher than the target maturity level, the VDA ISA cuts it back (the colours green, orange and red match with the colours used in the "Result" column, see figure 24).

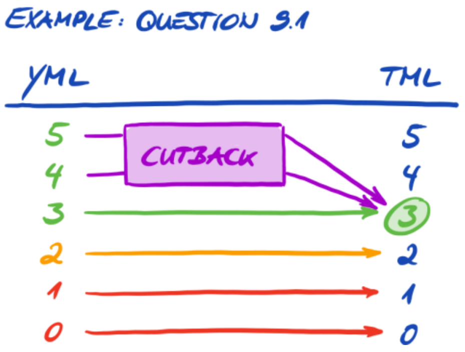


Figure 26: Cutback illustration with the colours used in the Excel sheet "Results"

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.

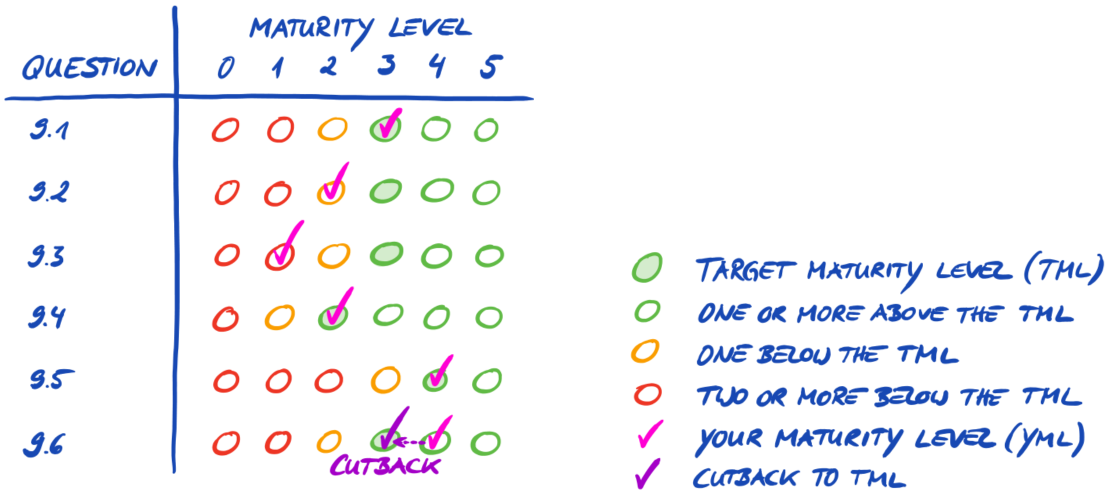

QUESTION
MATURITY LEVEL
0 1 2 3 4 5
9.1
9.2
9.3
9.4
9.5
9.6
CUTBACK
TARGET MATURITY LEVEL (TML)
ONE OR MORE ABOVE THE TML
ONE BELOW THE TML
TWO OR MORE BELOW THE TML
YOUR MATURITY LEVEL (YML)
CUTBACK TO TML

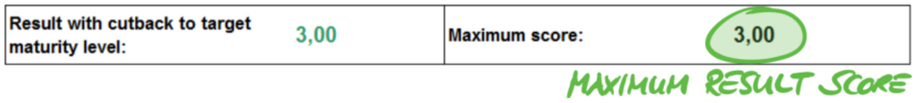
Figure 27: Maturity levels on question level

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 VDA ISA defines an "ideal" overall maturity level – the "maximum result score" (or "Maximum score", cell G14).



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

Figure 28: Maximum result score (Excel sheet "Results")

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 only “3.0” if all questions apply to your situation. As soon as a question is not applicable to your situation and its target maturity level is “2” or “4”, the average changes and the maximum result score is lower or higher than “3.0”.

Picking up a view shown further above (figure 27), you can see below what's put into the average for the maximum result score:

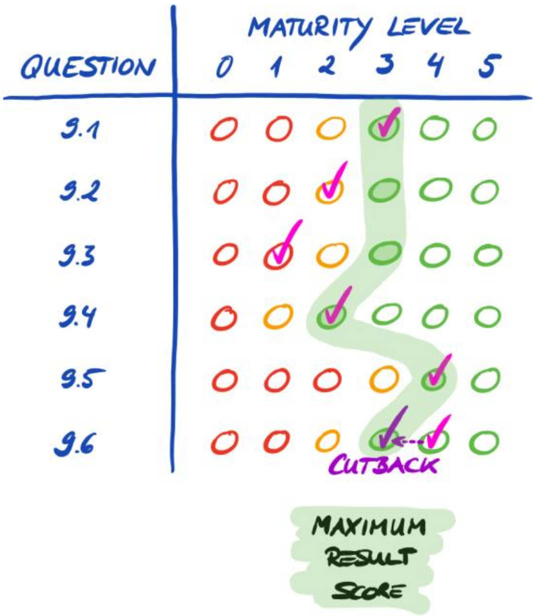
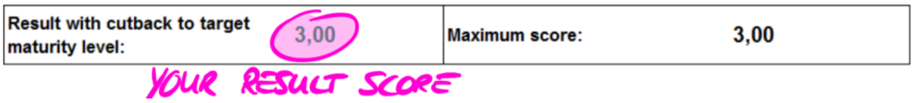


Figure 29: The maximum result score (on score level)

5.2.4.5 Your result (on score level)

Your overall result score (“Result with cutback to target maturity levels”, cell D14):

- 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 are able to receive TISAX labels.



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

Figure 30: Your result score (Excel sheet “Results”)

Again using a view shown further above (figure 27), you can see below what's put into the average for the result score:

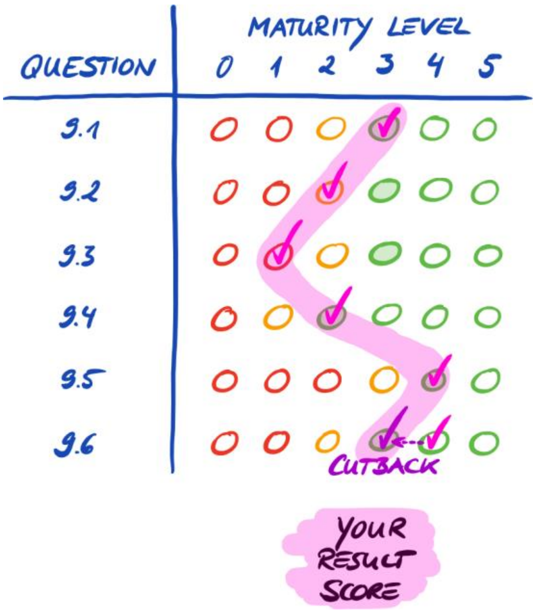


Figure 31: Your result score (on score level)

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 consider 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 in green (no orange, no red).

If not, you need to address your self-assessment result (please refer to section “5.2.5 Address the self-assessment result” on page 63).

Figure 32 shows the VDA ISA spider web diagram on the Excel sheet “Results”. 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 for receiving TISAX labels.

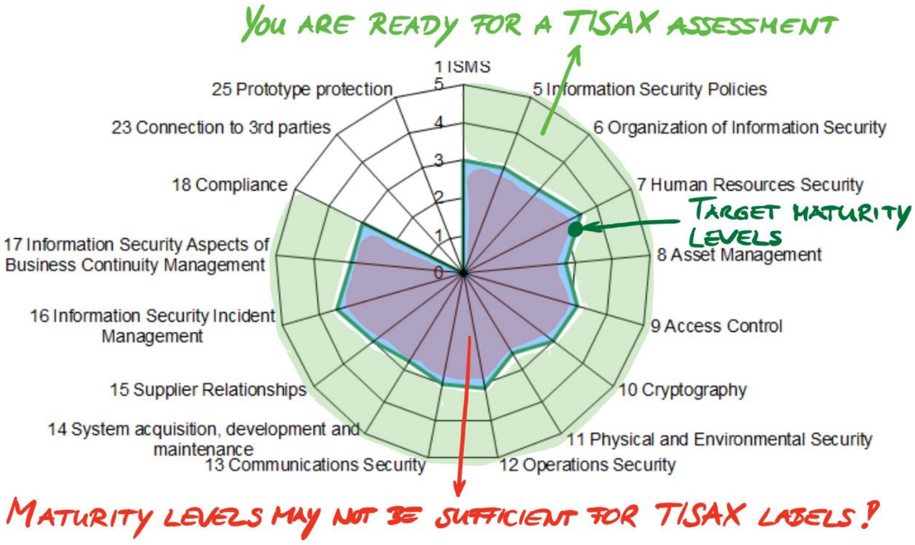


Figure 32: Screenshot: Target maturity level fulfilment in the VDA ISA spider web diagram (Excel sheet “Results”)

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

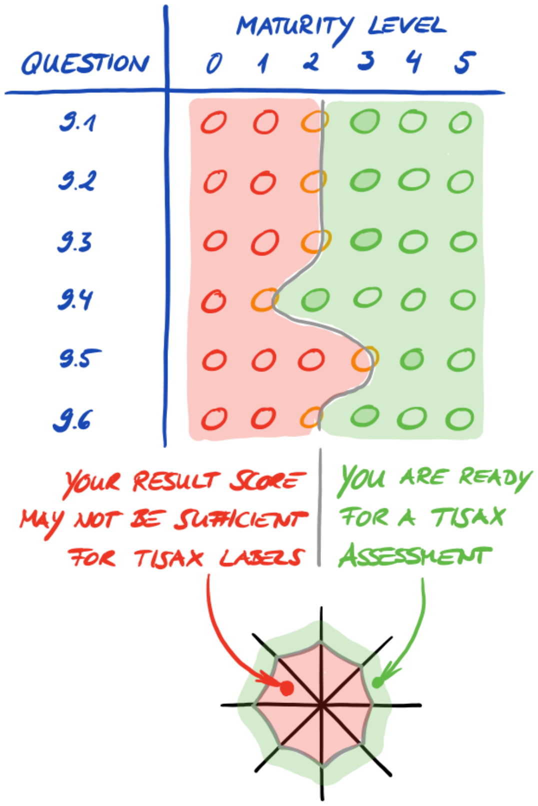

MATURITY LEVEL
QUESTION
0 1 2 3 4 5
9.1
9.2
9.3
9.4
9.5
9.6
YOUR RESULT SCORE MAY NOT BE SUFFICIENT FOR TISAX LABELS
YOU ARE READY FOR A TISAX ASSESSMENT

Figure 33: “Unfolding” the VDA 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 oblige them to consult. Please note that any audit provider doing consulting for you can't conduct TISAX assessments for you anymore.

⚠ 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 substantial project to get prepared for a TISAX assessment.

5.3 Audit provider selection

Only audit providers that we contracted can conduct TISAX assessments[27]. TISAX audit providers are only allowed to conduct TISAX assessments for you if they hadn't had any previous consulting assignments with you.

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

Please note:

Every assessment scope runs 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 "7.5.4 Assessment scope status "Approved" on page 94.

5.3.1 Contact information

Once you are registered, you can contact all TISAX audit providers and request offers. Their contact information is provided in the registration confirmation email you received[28] (please refer to section "4.5.8 Confirmation email" on page 41.

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 all 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 staff in many countries. Just request offers from all of them. There is no need to ask us which audit provider can conduct a TISAX assessment in country X.

5.3.3 Requesting offers

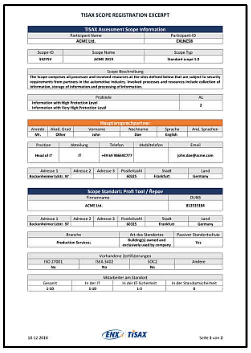
In order to allow our TISAX audit providers to precisely calculate the expected assessment efforts, you should include the following in your request:

- Your assessment objective(s)
  For more information on assessment objectives, please refer to section "4.3.3 Assessment objectives" on page 27.

[27] 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 to find out what is required to become a TISAX audit provider.

[28] Audit providers that are not included in our listing are not allowed to conduct TISAX assessments.

- Your self-assessment based on the VDA ISA
- Your ”TISAX Scope Excerpt”



TISAX SCOPE REGISTRATION EXCERPT

TISAX Assessment Scope Information	
Participant Name	Participant-ID
ACME Ltd.	CXLNC58

Scope-ID	Scope Name	Scope Typ
S3ZYXV	ACME 2019	Standard scope 1.0

Scope Beschreibung
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.

Prüfziele	AL
Information with High Protection Level Information with Very High Protection Level	2

Hauptansprechpartner					
Anrede	Akad. Grad	Vorname	Nachname	Sprache	And. Sprachen
Mr.	Other	John	Doe	English	

Position	Abteilung	Telefon	Mobiltelefon	Email
Head of IT	IT	+49 69 986692777		john.doe@acme.com

Adresse 1	Adresse 2	Adresse 3	Postleitzahl	Stadt	Land
Bockenheimer Ldstr. 97			60325	Frankfurt	Germany

Scope Standort: Profi Tool / Řepov	
Firmenname	DUNS
ACME Ltd.	812533184

Adresse 1	Adresse 2	Adresse 3	Postleitzahl	Stadt	Land
Bockenheimer Ldstr. 97			60325	Frankfurt	Germany

Branche	Art des Standortes	Passiver Standortschutz
Production Services;	Building(s) owned and exclusively used by company	Yes

Vorhandene Zertifizierungen			
ISO 27001	ISEA 3402	SOC2	Andere
No	No	No	

Mitarbeiter am Standort			
Gesamt	In der IT	In der IT-Sicherheit	In der Standortsicherheit
1-10	1-10	1-5	0

10.12.2018 Seite 1 von 2

Figure 34: Thumbnail of a scope excerpt (first page)

For more information, please refer to section “4.5.8 Confirmation email” on page 41.

Further notes:

- Impartiality is a key characteristic of our TISAX audit providers. They will ensure that no conflict of interest exits. 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.
- At this stage, you should not include any additional reference documents (as specified in the self-assessment). Later, you will be asked for these documents by the audit provider of your choice. You should prepare this document package while you are waiting for the responses of the audit providers.

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 sympathy, 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.
- Which assessments are included?
  For more information on assessments, please refer to section “5.4.2 TISAX assessment types and elements” on page 66.
  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.

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.[29]

5.4.2 TISAX assessment types and elements

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

- Initial assessment
- Corrective action plan assessment
- Follow-up assessment[30]

The initial assessment marks the start of the TISAX assessment process.

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 (at which point another initial assessment is required).

All TISAX assessments will be described in the coming sections.

Please note:

Every assessment runs through a life cycle.

For more information on the status of an assessment, please refer to section “7.6 Annexe: Assessment status” on page 95.

[29] In case of exiting the assessment process you won't receive TISAX labels.

[30] There is actually a fourth type: The “scope extension assessment”. As this is a special case, it is described in detail in the annexe in section “7.7.5 Additional location (scope extension assessment)” on page 96.

5.4.3 TISAX assessment elements

Each TISAX assessment consists of the following elements:

- Formal opening meeting[31, 32]
  - It aims to cover all organisational topics.
  - It does not necessarily have to be a physical meeting.
  - Topics can be covered in one pass 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[33]
  - 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 report”. You can voice objections if you think the audit provider misunderstood something.[34] Then the audit provider issues the final “TISAX report”.

All these elements will be described in the next sections.

5.4.4 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 does “conform” to all requirements, you pass the assessment and receive the TISAX labels that correspond with your assessment objectives.

[31] The formal *opening* meeting will only be described in detail for the initial assessment. For the other TISAX assessments, your audit provider will schedule and shape these meetings.

[32] Some audit providers may use the term “kickoff meeting” synonymously for “formal opening meeting”.

[33] The formal *closing* meeting will only be described in detail for the initial assessment. For the other TISAX assessments, your audit provider will schedule and shape these meetings.

[34] If a dispute can't be solved, you can escalate the issue. Please contact us for further details.

If your approach does *not* conform to a given requirement, the audit provider differentiates two types of “non-conformity”:

a) *Minor* non-conformity

This applies when the non-conformity neither questions the overall effectiveness of your information security management system nor creates a significant information security risk.

Examples: Isolated or sporadic mistakes, implementation deficits

b) *Major* non-conformity

This applies when the non-conformity creates doubts in the overall effectiveness of your information security management system or if it causes significant information security risks.

Examples: 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

Please note:

For the assessment result, everything below full or ideal conformity to the requirements is called a finding. TISAX differentiates four types of findings:

- Observation
- Room for improvement
- Minor non-conformity
- Major non-conformity

Only the two non-conformities are relevant for the assessment result.

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 “5.4.13 TISAX labels” on page 78.

5.4.5 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 formal opening meeting.

A good preparation of the 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.

5.4.6 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. Maximum validity period of three years for TISAX labels
2. Maximum duration of nine months for the entire TISAX assessment process

   This period starts with the initial assessment. It ends with the last follow-up assessment.

   This is a hard deadline. If you don't successfully complete the assessment process within this period, you won't receive TISAX labels.

The periods both start on the day of the closing meeting.

5.4.6.1 The first formal opening meeting

Like all TISAX assessments, the initial assessment starts with a formal opening meeting. Unlike for the other TISAX assessment types, this meeting covers the most topics as it is the start of the interaction with your audit provider. The formal opening meeting is usually done with a conference call or web conference.

The purpose of this meeting is to:

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

Assessment prerequisites to be checked are:

- Do you have a valid TISAX registration?
- Is the contract between you and your audit provider signed?

Assessment planning includes:

- Assessment scope verification
  - Is your scope registered and appropriate?[35]
- Assessment objective check
  - Does the assessment objective match your own and/or your partner's requirements?
- Staff on your side
  - Based on their ISMS-related roles in your company, who must be available for interviews (by phone, or in person during on-site assessments)?
- Communication between you and the audit provider
  - How will you exchange confidential information? You will send confidential documentation to the audit provider and he will send confidential assessment reports.
  - Who is to be included in any communication?
  - If applicable: How will you conduct conference calls and web conferences for interviews?
- Key assessment topics
  - Based on your self-assessment the audit provider will present the key topics he will focus on.
- Time planning
  - Deadlines for documentation you have to send (including your self-assessment based on the VDA ISA and related documentation, if not sent already)
  - Appointments for interviews and on-site inspections (if applicable)
  - Deadlines for assessment reports (draft and final)

5.4.6.2 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[36].

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

5.4.6.3 Closing meeting

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

5.4.6.4 TISAX report

After the closing meeting, the audit provider prepares and sends you the draft version of the “TISAX report”. You can voice objections if you think the audit provider misunderstood something.[37] Then the audit provider issues the “TISAX report”.

[35] Changes to the scope are still possible at this stage.

[36] For more information on audit methods and intensities, please refer to section “4.3.3.6 Protection needs and assessment levels” on page 32.

[37] If a dispute can't be solved, you can escalate the issue. Please contact us for further details.

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 “5.4.8.4 Temporary TISAX labels” on page 73.

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”.

5.4.7 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 your “corrective action plan” for whether it is appropriate (see next section).

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

- 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.

5.4.8 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 report”.

This assessment usually doesn't take long. It can be a physical meeting as well as a conference call or web conference.

5.4.8.1 Prerequisites for a corrective action plan assessment

The prerequisites for a “corrective action plan assessment” are either:

- a recent[38] initial assessment with non-conformities
- or a “corrective action plan” that already has been assessed, but did not fulfil the requirements.

5.4.8.2 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.

5.4.8.3 Corrective action plan requirements

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

- Measures are appropriate
- Critical risks are mitigated with appropriate compensating measures[39]
- 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

[38] The period between initial assessment and corrective action plan assessment can't be longer than 9 months.

[39] 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.

5.4.8.4 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”.

Regarding the validity period, temporary TISAX labels:

- expire nine months after the closing meeting of the initial assessment.
- are valid until all non-conformities are resolved.
  - This is established in the follow-up assessment and documented in the follow-up assessment report.
- can't be renewed.

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”.

5.4.9 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.

5.4.9.1 Timing

Your audit provider can conduct the follow-up assessment(s) within up to nine months after the conclusion of the initial assessment[40].

[40] 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”.

5.4.9.2 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.

5.4.9.3 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[41]. The reason is that you want to have enough buffer time to address any minor findings identified during a follow-up assessment.

[41] In theory, this can be 9 month after the conclusion of the initial assessment.

5.4.10 TISAX assessment process diagram

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

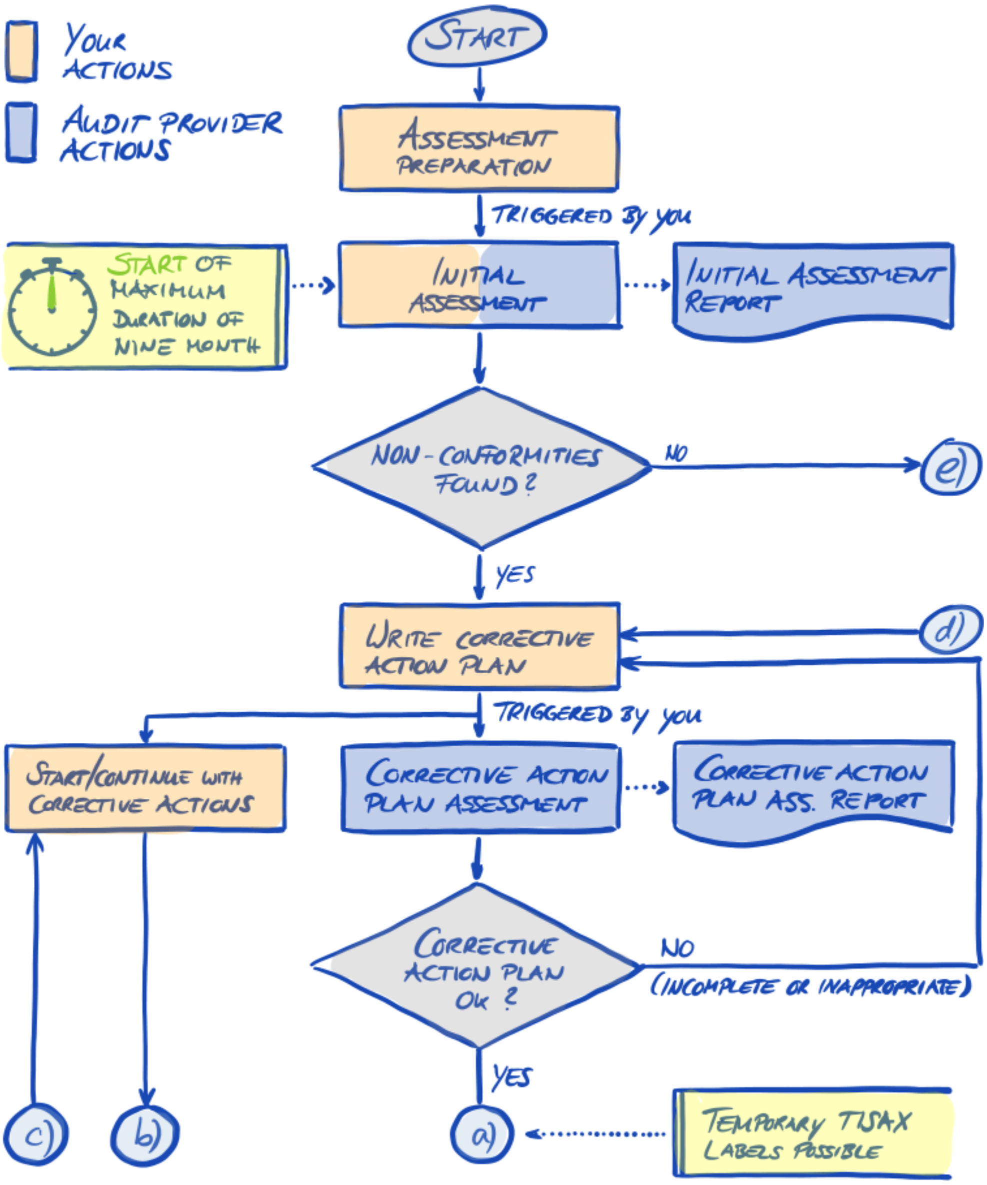

YOUR ACTIONS
AUDIT PROVIDER ACTIONS
START
ASSESSMENT PREPARATION
TRIGGERED BY YOU
START OF MAXIMUM DURATION OF NINE MONTH
INITIAL ASSESSMENT
INITIAL ASSESSMENT REPORT
NON-CONFORMITIES FOUND?
NO
e)
YES
WRITE CORRECTIVE ACTION PLAN
d)
TRIGGERED BY YOU
START/CONTINUE WITH CORRECTIVE ACTIONS
CORRECTIVE ACTION PLAN ASSESSMENT
CORRECTIVE ACTION PLAN ASS. REPORT
CORRECTIVE ACTION PLAN OK?
NO
(INCOMPLETE OR INAPPROPRIATE)
YES
c)
b)
a)
TEMPORARY TISAX LABELS POSSIBLE

Figure 35: TISAX assessment process diagram (part 1/2)

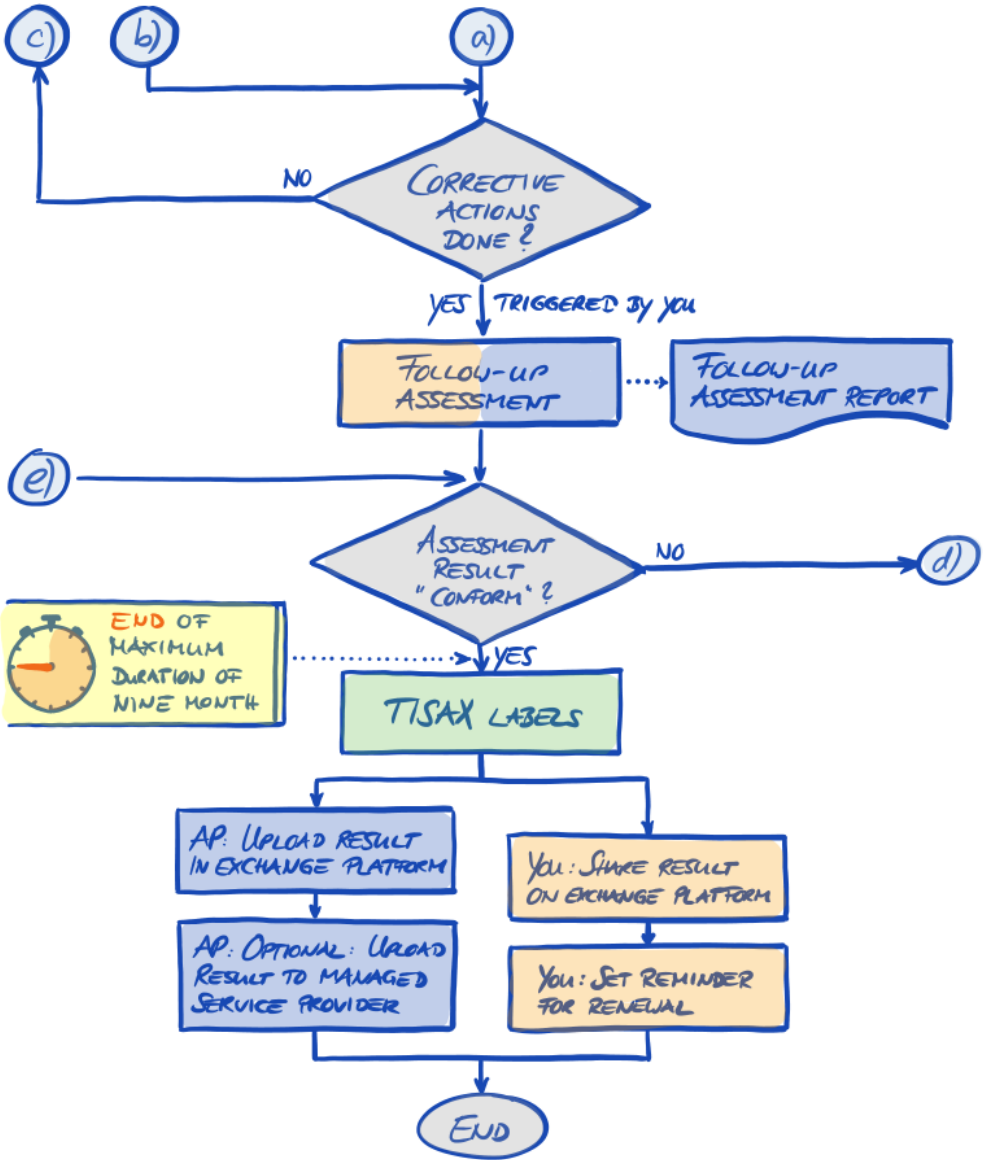

c)
b)
a)
NO
CORRECTIVE ACTIONS DONE ?
YES
TRIGGERED BY YOU
FOLLOW-UP ASSESSMENT
FOLLOW-UP ASSESSMENT REPORT
e)
ASSESSMENT RESULT "CONFORM" ?
NO
d)
END OF MAXIMUM DURATION OF NINE MONTH
YES
TISAX LABELS
AP: UPLOAD RESULT IN EXCHANGE PLATFORM
YOU: SHARE RESULT ON EXCHANGE PLATFORM
AP: OPTIONAL: UPLOAD RESULT TO MANAGED SERVICE PROVIDER
YOU: SET REMINDER FOR RENEWAL
END

Figure 36: TISAX assessment process diagram (part 2/2)

5.4.11 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 report.

This is what the Assessment ID looks like:

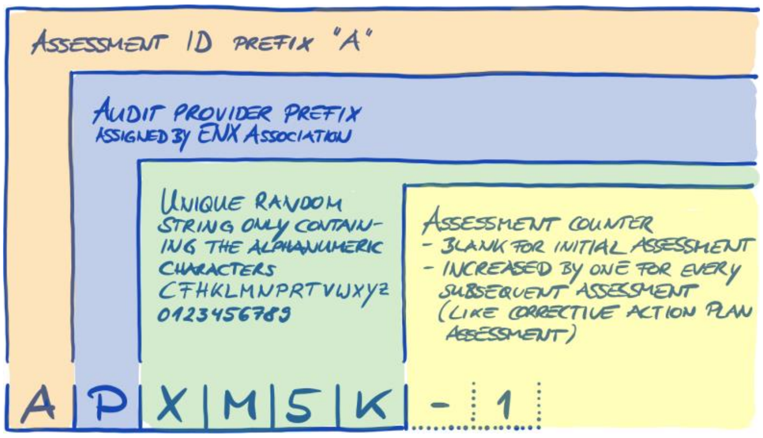

ASSESSMENT ID PREFIX "A"
AUDIT PROVIDER PREFIX
ASSIGNED BY ENX ASSOCIATION
UNIQUE RANDOM STRING ONLY CONTAINING THE ALPHANUMERIC CHARACTERS
CFHKLMNPRTVWXYZ
0123456789
ASSESSMENT COUNTER
- BLANK FOR INITIAL ASSESSMENT
- INCREASED BY ONE FOR EVERY SUBSEQUENT ASSESSMENT (LIKE CORRECTIVE ACTION PLAN ASSESSMENT)
A P X M 5 K - 1

Figure 37: Format of the Assessment ID

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

5.4.12 TISAX report

The “TISAX 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 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[42]

The “TISAX report” always has the same structure[43]. 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 report as it always contains the content of its older version(s).

The “TISAX 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 report you want to share with your partner or any other participant. The structure of the TISAX report is designed to enable this kind of selective sharing. Each section expands the level of detail.

[42] Actually, there is a fourth type: The “scope extension assessment report”. As this is a special case, it is described in detail in section “7.7.5 Additional location (scope extension assessment)” on page 96.

[43] The “TISAX report” is based on a template that all TISAX audit providers are obliged to use.

Here is what the structure of the "TISAX 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: Overall assessment result

  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: Detailed assessment results

  Detailed description of all findings, corresponding risk assessment results, required measures, implementation period
- E: Maturity levels of VDA ISA (result tab of VDA ISA)

  Maturity level for each requirement

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

5.4.13 TISAX labels

We briefly touched on this topic in the registration preparation section (page 30). As explained, what once was an assessment objective now became a TISAX label.

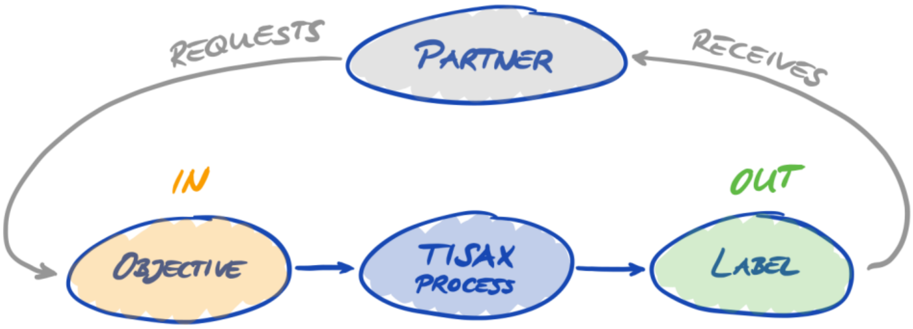


Figure 38: Assessment objectives and TISAX labels

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.

5.4.13.1 TISAX label hierarchy

The mapping between any assessment objective and the corresponding TISAX labels is pretty straight forward. 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 an extension of “Info high”, you automatically receive the TISAX label “Info high”, too.

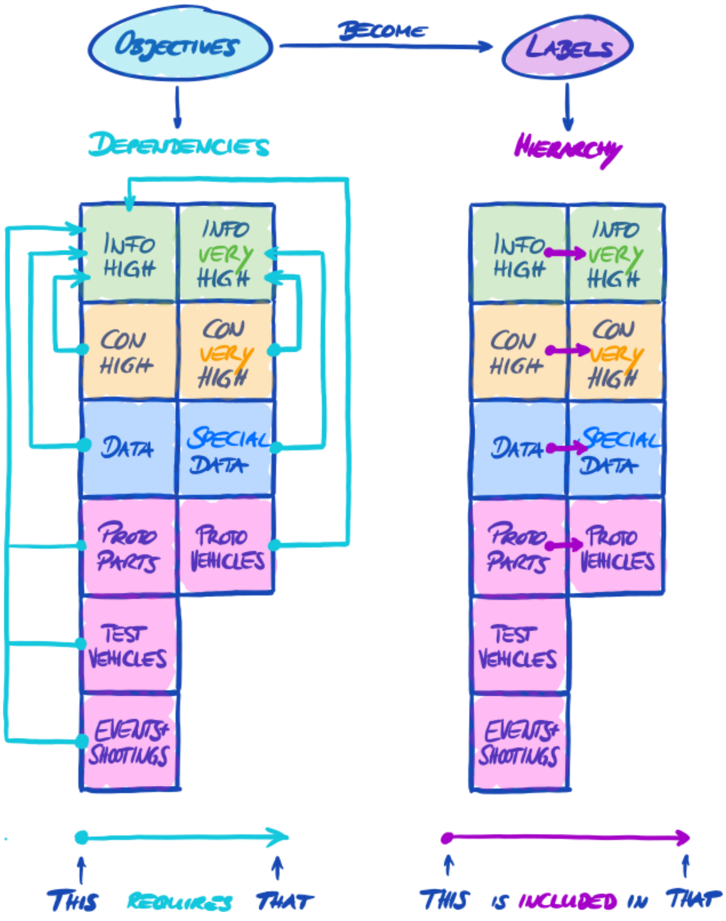


Figure 39: TISAX assessment objectives and TISAX labels (dependencies and hierarchy)

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'“.

5.4.13.2 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 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 sections “7.7.4 Relocations” and “7.7.5 Additional location (scope extension assessment)” on page 98.)

Please note:

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

5.4.13.3 Renewal of TISAX labels

To keep your TISAX labels long-term, you need to renew 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:

If always having valid TISAX labels during the relationship with your partner is a requirement, we strongly advise you to put a reminder in your calendar that triggers 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 may have gone through the TISAX process up to here, but so far your partner still has not seen any “proof” that your information security management system is capable to protect 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 provides the exchange platform.

Your audit provider will upload the first two sections (A and B) of your TISAX 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:

https://portal.enx.com

6.3 General prerequisites

You can only share your assessment result with your partner 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 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 runs 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 “7.5.6 Assessment scope status “Active” on page 94.

Please note:

If you are a partner of Volkswagen AG, Audi AG or Porsche AG, and if “operational services GmbH & Co. KG” started the assessment between the years 2015 and 2017, you can request the acceptance of your “Volkswagen legacy assessment result” in TISAX.

For instructions on how to request the acceptance, please refer to section “7.8 Annexe: Volkswagen legacy assessments” on page 98.

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

1. Log in to the ENX portal.
2. Go to the main navigation bar and select “MY ENX PORTAL”.
3. From the dropdown menu, select “MY SCOPES AND ASSESSMENTS”.
4. Go to the table at the end of the page 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 accidently created a publication or sharing permission, please contact us immediately.

6.5 Sharing levels

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

	Main sections of the TISAX report	Sharing levels on the exchange platform
1	A: Assessment-related information	
2	B: Overall assessment result	
3	C: Assessment result summary	
4	D: Detailed assessment results	
5	E: Maturity levels of VDA ISA (result tab of VDA ISA)	

Table 12: Main sections of the TISAX 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 report, please refer to section “5.4.12 TISAX report” on page 77.

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: Assessment Summary

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

Important note:
You can only publish your assessment result if the prerequisites described in section “6.3 General prerequisites” on page 81 are fulfilled.

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

1. Log in to the ENX portal.
2. Go to the main navigation bar and select “MY ENX PORTAL”.
3. From the dropdown menu, select “MY SCOPES AND ASSESSMENTS”.
4. Go to the table at the end of the page 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 “TISAX Assessment Results & Sharing”.
8. Go to the section “Publication”, open the drop-down menu and select the desired sharing level (see recommendation above).

Please note:
The assessment results are only published on the exchange platform. They can only be accessed by other TISAX participants. 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:

- A + Labels
- A + Labels + B: Overall Assessment Result
- A + Labels + B + C: Assessment Result Summary
- A + Labels + B + C + D: Detailed Assessment Results
- A + Labels + B + C + D + E: Maturity Level according to VDA ISA

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.[44]
- You need to pay the fee (if applicable).

⚠ Important note:

You can only share your assessment result if the general prerequisites described in section “6.3 General prerequisites” on page 81 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.
2. Go to the main navigation bar and select “MY ENX PORTAL”.
3. From the dropdown menu, select “MY SCOPES AND ASSESSMENTS”.
4. Go to the table at the end of the page 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 “TISAX Assessment Results & Sharing”.
8. Go to the section “Sharing Permission” and click the button “Share”.
9. Enter your partner's Participant ID.
10. Select the desired sharing level.
11. Click the button “Next”.
12. Read and understand the instructions regarding the permanence of the sharing permission.
13. Mark the two “confirm” check boxes.
14. Click the button “Submit”.

[44] 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 directly contacting him.

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[45].

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.

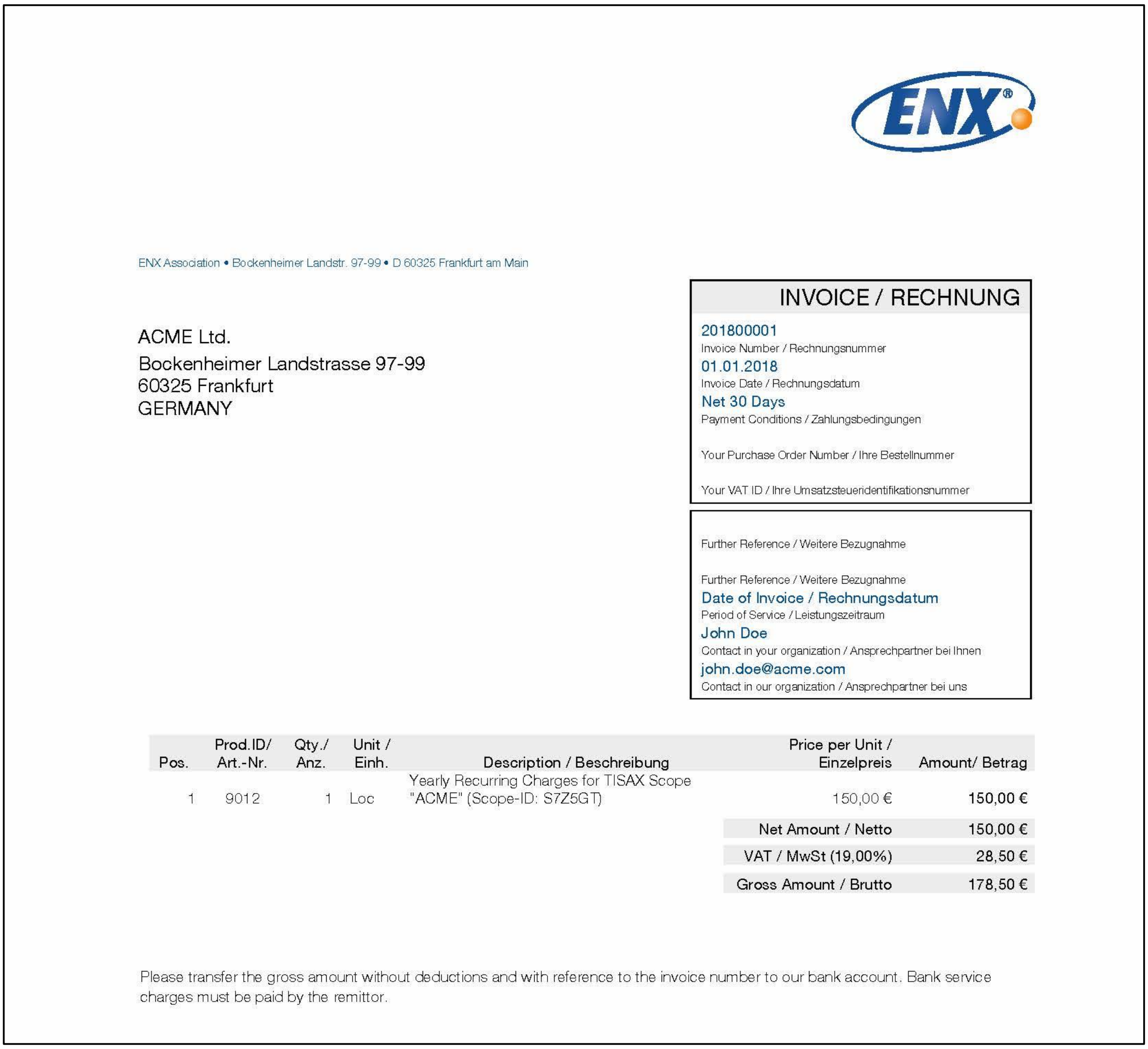
[45] Your partner has to log into the portal and actively look up your shared assessment result. Your partner doesn't receive an automated notification about new shared assessment results.

7 Annexes

7.1 Annexe: Example invoice

This is an example of the invoice we send.

For more information, please refer to section “4.3.4 Fee” on page 36.



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

ACME Ltd.
Bockenheimer Landstrasse 97-99
60325 Frankfurt
GERMANY

INVOICE / RECHNUNG

201800001
Invoice Number / Rechnungsnummer
01.01.2018
Invoice Date / Rechnungsdatum
Net 30 Days
Payment Conditions / Zahlungsbedingungen

Your Purchase Order Number / Ihre Bestellnummer

Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

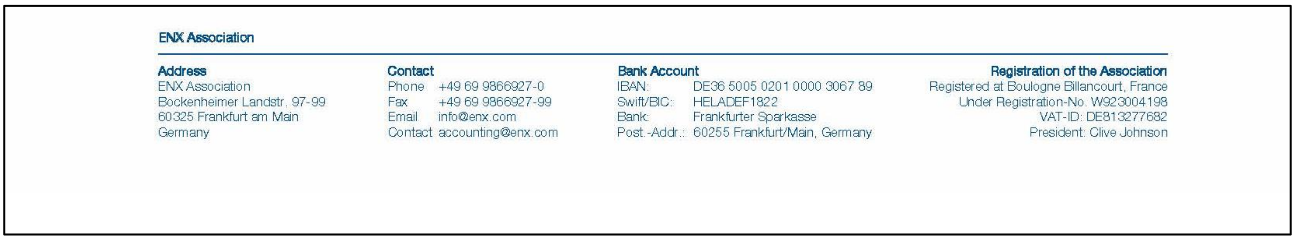
Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
Period of Service / Leistungszeitraum
John Doe
Contact in your organization / Ansprechpartner bei Ihnen
john.doe@acme.com
Contact in our organization / Ansprechpartner bei uns

Pos.	Prod.ID/ Art.-Nr.	Qty./ Anz.	Unit / Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9012	1	Loc	Yearly Recurring Charges for TISAX Scope "ACME" (Scope-ID: S7Z5GT)	150,00 €	150,00 €
					Net Amount / Netto	150,00 €
					VAT / MwSt (19,00%)	28,50 €
					Gross Amount / Brutto	178,50 €

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 remittor.

[...]



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 accounting@enx.com

Bank Account
IBAN: DE36 5005 0201 0000 3067 89
Swift/BIC: HELADEF1822
Bank: Frankfurter Sparkasse
Post.-Addr.: 60255 Frankfurt/Main, Germany

Registration of the Association
Registered at Boulogne Billancourt, France
Under Registration-No. W923004198
VAT-ID: DE813277682
President: Clive Johnson

7.2 Annexe: 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” on page 41.

Subject: TISAX Registration

Dear [...],

thank you for the registration documents. I have carried out your registration. Attached you can find a data base excerpt about your recorded information. The next step in the TISAX process will be to request quotes for an assessment from TISAX audit providers. Currently the following audit providers can provide TISAX Assessments:

[Current list of TISAX audit providers and their sales contacts]

In your request, please inform the audit services provider about the information on the assessment scope , the assessment objective (i.e. “Handling of Information with High Protection needs” or “Handling of Prototypes with Very High Protection needs”).

Please verify if the information in our database is correctly transcribed. If there are any mistakes, please give me a hint and I will contact it.

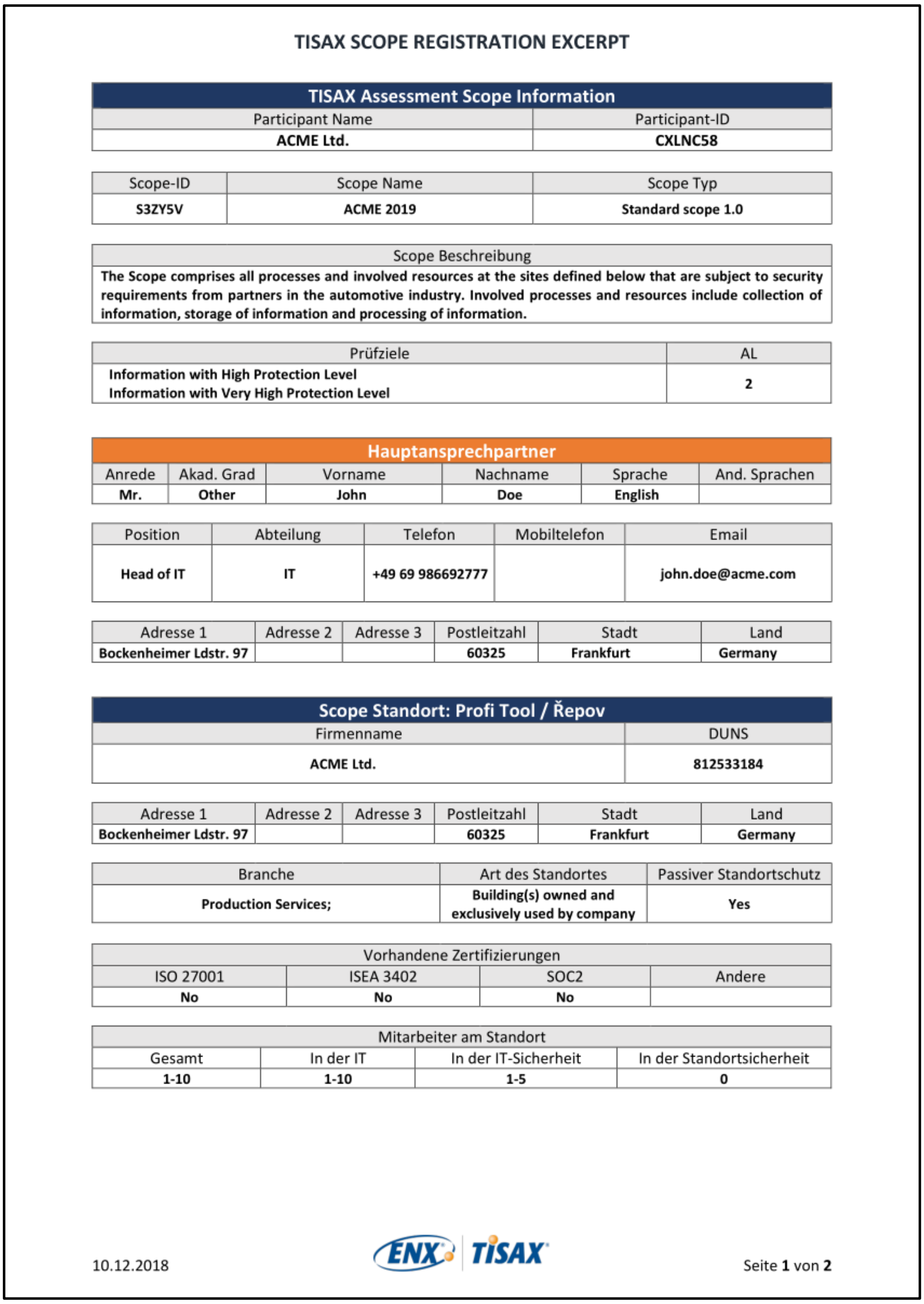
If you have any further questions, please don't hesitate to contact us.

Kind regards,
[...]

7.3 Annexe: 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” on page 41.



TISAX SCOPE REGISTRATION EXCERPT

TISAX Assessment Scope Information

Participant Name	Participant-ID
ACME Ltd.	**CXLNC58**

Scope-ID	Scope Name	Scope Typ
S3ZY5V	**ACME 2019**	**Standard scope 1.0**

Scope Beschreibung
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.

Prüfziele	AL
Information with High Protection Level **Information with Very High Protection Level**	**2**

Hauptansprechpartner

Anrede	Akad. Grad	Vorname	Nachname	Sprache	And. Sprachen
Mr.	**Other**	**John**	**Doe**	**English**	

Position	Abteilung	Telefon	Mobiltelefon	Email
Head of IT	**IT**	**+49 69 986692777**		**john.doe@acme.com**

Adresse 1	Adresse 2	Adresse 3	Postleitzahl	Stadt	Land
Bockenheimer Ldstr. 97			**60325**	**Frankfurt**	**Germany**

Scope Standort: Profi Tool / Řepov

Firmenname	DUNS
ACME Ltd.	**812533184**

Adresse 1	Adresse 2	Adresse 3	Postleitzahl	Stadt	Land
Bockenheimer Ldstr. 97			**60325**	**Frankfurt**	**Germany**

Branche	Art des Standortes	Passiver Standortschutz
Production Services;	**Building(s) owned and exclusively used by company**	**Yes**

Vorhandene Zertifizierungen			
ISO 27001	ISEA 3402	SOC2	Andere
No	**No**	**No**	

Mitarbeiter am Standort			
Gesamt	In der IT	In der IT-Sicherheit	In der Standortsicherheit
1-10	**1-10**	**1-5**	**0**

10.12.2018

Seite **1** von **2**

7.4 Annexe: Participant status

7.4.1 Participant status overview

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:

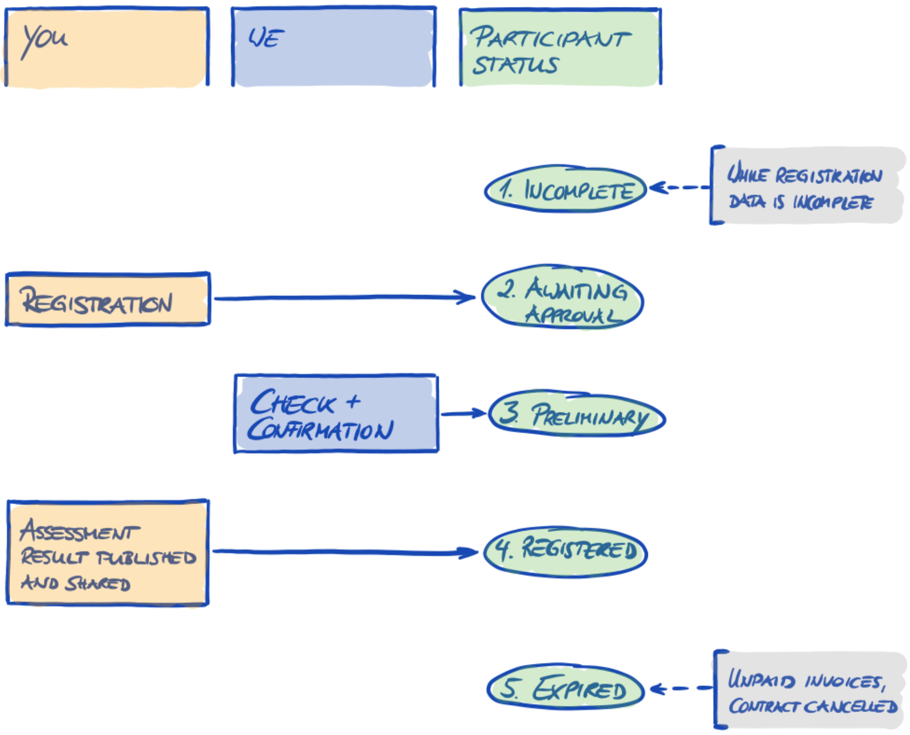


Figure 40: Participant status overview

7.4.2 Participant status "Incomplete"

Status	Situation	Your next action	Our next action	Next status
Incomplete	You have not completed the TISAX registration. Either you have not accepted the general terms and conditions. Or you have not specified the main participant location. Or you have not assigned a main participant contact. Or any other information we require is missing.	Continue at 🇬🇧 https://portal.enx.com/	We will send you a reminder by email (usually within a few days).	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	You have successfully completed the TISAX assessment process and received TISAX labels. You have published and shared your assessment result. You only receive TISAX labels when you successfully passed the TISAX assessment process. In the ENX portal, this is reflected by having an assessment scope with the assessment scope status "Active".	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 of 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	You have not paid the fee. Or you or we have cancelled our mutual contract (the GTCs).	None	None	n/a

7.5 Annexe: Assessment scope status

7.5.1 Assessment scope status overview

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 Annexe: Assessment status" on page 95.

Your “assessment scope status” can be:

1. Incomplete
2. Awaiting approval
3. Approved
4. Registered
5. Active
6. 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:

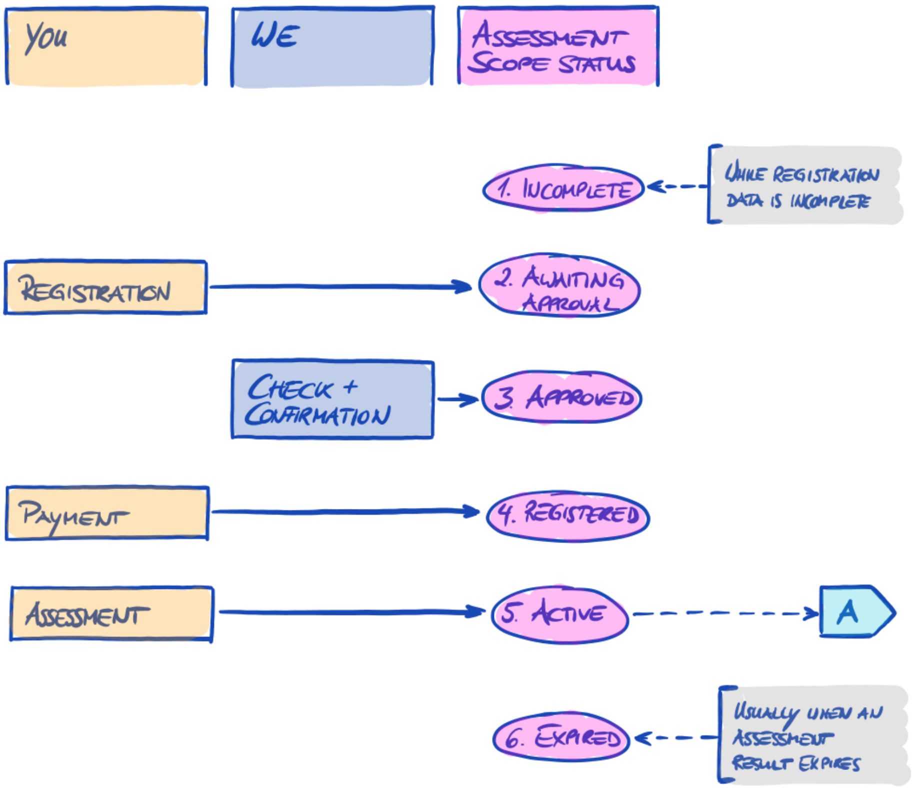


Figure 41: Assessment scope status overview

The off-page reference “A” in figure 41 links the assessment scope status “Active” with the “assessment status”. For more information on the “assessment status”, please refer to section “7.6 Annexe: Assessment status” on page 95.

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 https://portal.enx.com/	We will send you a reminder by email (usually within a few days).	Awaiting approval

For more information on where this status is playing a role, please refer to section “4.5.7 Assessment scope registration” on page 40.

7.5.3 Assessment scope status “Awaiting approval”

Status	**Situation**	**Your next action**	**Our next action**	**Next status**
Awaiting 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.	Approved

For more information on where this status is playing a role, please refer to section “4.5.7 Assessment scope registration” on page 40.

7.5.4 Assessment scope status "Approved"

Status	Situation	Your next action	Our next action	Next status
Approved	Your assessment scope registration is complete and approved. You have received our confirmation email and the "TISAX Scope Excerpt".	Pay the fee (if applicable). Request offers from our TISAX audit providers. From the status "Approved" onwards, you: ▪ can start sharing some assessment-related information with your partner.[46] ▪ can pre-configure the publication of your assessment result (this will only become effective once your assessment scope status changes to "Active".	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" on page 41.

7.5.5 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

7.5.6 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

[46] While at assessment scope status "Approved" 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.

For more information on publishing and sharing, please refer to section “6 Exchange (Step 3)” on page 81.

7.5.7 Assessment scope status “Expired”

Status	Situation	Your next action	Our next action	Next status
Expired	Either: ▪ 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 (3 years), ▪ or you had major changes to the assessment scope (example: all locations in an assessment scope do not belong to your company anymore).	Start a new assessment scope registration.	None	Incomplete or Awaiting approval

7.6 Annexe: Assessment status

7.6.1 Assessment status overview

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 Annexe: Assessment scope status” on page 91.

Your “assessment status” can be:

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

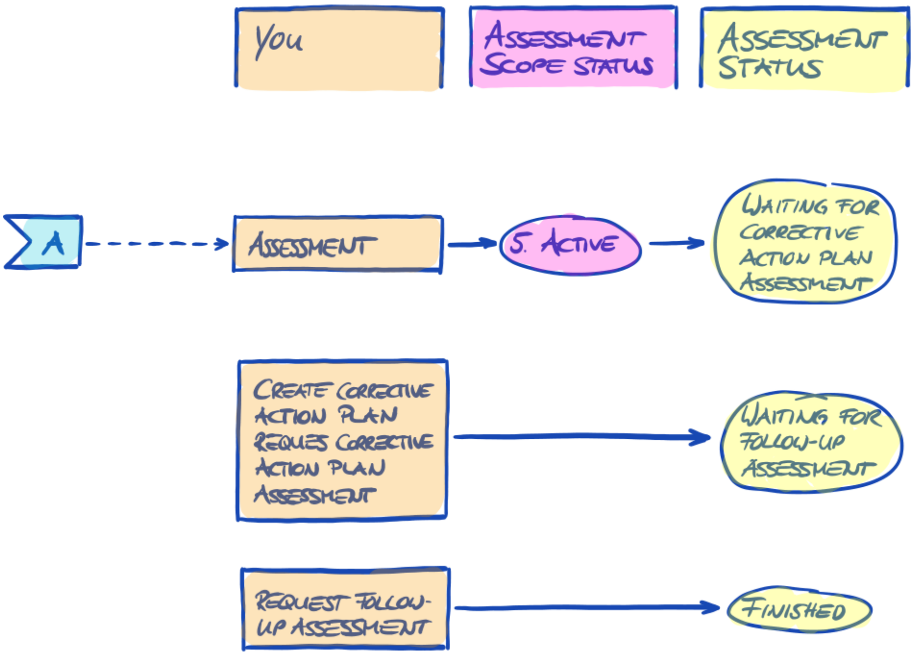

YOU
ASSESSMENT SCOPE STATUS
ASSESSMENT STATUS
A
ASSESSMENT
5. ACTIVE
WAITING FOR CORRECTIVE ACTION PLAN ASSESSMENT
CREATE CORRECTIVE ACTION PLAN
REQUES CORRECTIVE ACTION PLAN ASSESSMENT
WAITING FOR FOLLOW-UP ASSESSMENT
REQUEST FOLLOW-UP ASSESSMENT
FINISHED

Figure 42: Assessment status overview

The off-page reference “A” in figure 42 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 Annexe: Assessment scope status” on page 91.

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	Waiting for corrective action plan assessment (if applicable)

7.6.3 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. 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 assessment (if applicable)

7.6.4 Assessment status “Waiting for follow-up assessment”

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

7.6.5 Assessment status “Finished”

Status	Situation	Your next action	Our next action	Next status
Finished	Your audit provider conducted an follow-up assessment and issued the TISAX report.	Publish and share your assessment result.	None	n/a

7.7 Annexe: Participant data life cycle management

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

7.7.1 Change of company name

If you want to change your company's name, please contact us.

7.7.2 Change 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

7.7.3 Lost access to participant data (ENX portal)

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

7.7.4 Relocations

If only the name of a street is officially changed, your company's main participant contact just needs to contact us. We will update the location data accordingly.

But if one of your locations relocates to a new address, you need to:

1. extend the assessment scope.
   Take the steps described in section "7.7.5 Additional location (scope extension assessment)" on page 98.
2. send us an email to let us know the old location is no longer part of your company.
   We will update the assessment scope data accordingly. We will send you a confirmation.

7.7.5 Additional location (scope extension assessment)

If you open a new location during the validity period of your existing TISAX labels, you need to request a "scope extension assessment" from your audit provider. You can't select another audit provider to conduct a "scope extension assessment". The assessment is similar to the other 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.

7.8 Annexe: Volkswagen legacy assessments

Before TISAX existed, Volkswagen had its own information security assessment process. The company "operational services" conducted these assessments on behalf of Volkswagen[47].

If you are a partner of Volkswagen AG, Audi AG or Porsche AG, and if "operational services GmbH & Co. KG" started the assessment between the years 2015 and 2017, you can request the acceptance of your "Volkswagen legacy assessment result" in TISAX.

In order to be able to share your "Volkswagen legacy assessment result"[48] in TISAX, you need to:

1. use this web page as entry point for a regular online registration:

   🇬🇧 https://enx.com/tisax/volkswagen-legacy-assessment-en.html

   🇩🇪 https://enx.com/tisax/volkswagen-legacy-assessment.html

   For further information on the online registration process, please refer to section "4 Registration (Step 1)" on page 15.
2. request "operational services" to inform us about your "Volkswagen legacy assessment result".

[47] Please note that "operational services GmbH & Co. KG" is now also a TISAX audit provider.

[48] A German term used for "Volkswagen legacy assessment result" is "Altfreigabe".

You may want to send your request to “fmb-informationssicherheit-partnerfirmen@o-s.de”.

8 Document history

Version	Notes
2.1.2	• Formal limit for "distance" between "your result score" and "maximum result score" corrected from 25% to 30%
2.1.1	• "TISAX-accredited audit provider" renamed to "TISAX audit provider")
2.1	• 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 VDA 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