Simplified Group Assessment

An addendum to the TISAX Participant Handbook for TISAX participants with many locations and a centralised and highly developed ISMS
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: 2018-12-10, Version: 1.0
Classification: Public, ENX doc ID: 603

Copyright notice
All rights reserved by ENX Association.
ENX, TISAX, and their respective logos are registered trademarks of ENX Association.
Cover photo by Jon Jonckers (jjonckers@gmail.com)
Third-party trademarks mentioned are the property of their respective owners.
# Table of contents

1 Overview .................................................................................................................................................. 5

1.1 Purpose ............................................................................................................................................... 5

1.2 Scope .................................................................................................................................................. 5

1.3 Audience ............................................................................................................................................ 5

1.4 Structure ............................................................................................................................................ 5

1.5 How to use this document .................................................................................................................. 5

1.6 Contact us ......................................................................................................................................... 6

2 Introduction ........................................................................................................................................... 7

3 Applicability .......................................................................................................................................... 9

3.1 Minimum number of locations in the assessment scope ........................................................................ 9

3.2 Centralised and highly developed ISMS ............................................................................................ 9

4 Considerations ...................................................................................................................................... 10

4.1 Pros .................................................................................................................................................. 10

4.2 Cons .................................................................................................................................................. 11

4.3 Further considerations ....................................................................................................................... 11

4.4 Comparison with regular process .................................................................................................... 13

5 Registration ......................................................................................................................................... 14

5.1 Preparation ....................................................................................................................................... 14

5.1.1 Applicability check ....................................................................................................................... 14

5.1.2 Scoping ....................................................................................................................................... 14

5.1.3 Registration fee ............................................................................................................................. 15

5.2 Online registration process .............................................................................................................. 15

6 Assessment .......................................................................................................................................... 17

6.1 VDA ISA self-assessment .................................................................................................................. 17

6.2 Requesting offers from TISAX-accredited audit providers ............................................................... 18

6.3 Assessment process .......................................................................................................................... 19

6.3.1 Location classes and check types .................................................................................................. 19

6.3.2 Precondition check ....................................................................................................................... 20

6.3.3 Sample checks ................................................................................................................................ 20

6.3.4 Simplified checks ........................................................................................................................... 21

6.3.5 Sample size .................................................................................................................................... 21

6.3.6 Sample selection ........................................................................................................................... 22
6.3.7 Assessment levels .................................................................................................................. 22
6.3.8 Conformity ........................................................................................................................... 24
6.3.9 Process duration ..................................................................................................................... 25
6.3.10 TISAX report ........................................................................................................................ 25

7 Exchange ........................................................................................................................................ 26

8 Lifecycle management ...................................................................................................................... 27
  8.1 Additional locations (scope extension assessment) ................................................................. 27
  8.2 Removing locations ..................................................................................................................... 28

List of tables
Table 1: Differences between the regular process and the simplified group assessment process .................. 13
Table 2: Example table for the scoping steps ..................................................................................... 15
Table 3: The six additional VDA ISA requirements for simplified group assessments ........................... 17
Table 4: Location classes and check types .......................................................................................... 19
Table 5: Check type differences ........................................................................................................ 20
Table 6: Examples for sample sizes .................................................................................................... 21
Table 7: Assessment level and locality for each location class ............................................................. 23

List of figures
Figure 1: The simplified group assessment in a nutshell ..................................................................... 7
Figure 2: Minimum number of locations in the assessment scope ....................................................... 9
Figure 3: Effort comparison between the simplified group assessment ("SGA") and the regular process ("Reg") .......... 10
Figure 4: Simplified group assessment process: Only the assessment step is different than in the regular process ...... 13
Figure 5: Where the additional requirements dock to in the VDA ISA document ................................. 18
Figure 6: The additional requirements as if they were included in the VDA ISA document ..................... 18
Figure 7: The location classes .......................................................................................................... 19
Figure 8: The location classes and check types .................................................................................. 19
Figure 9: The sample size diagram .................................................................................................... 22
Figure 10: Decision tree for determining the check type for new locations ...................................... 27
1 Overview

1.1 Purpose

For companies with many locations, the regular TISAX assessment process can be quite extensive. Under certain conditions we offer an alternative – the “simplified group assessment” (SGA). The simplified group assessment is a special case of the TISAX assessment process. If the preconditions are fulfilled, it can reduce the efforts compared to the regular TISAX assessment process.

This special TISAX assessment process is designed for companies with at least three locations and a centralised, highly developed information security management system (ISMS).

The purpose of this addendum is to describe when you can benefit from the simplified group assessment and how to get through the special assessment process.

1.2 Scope

This addendum applies to the TISAX assessment process “simplified group assessment”. It contains all you need to know to run through this special assessment process.

1.3 Audience

You are the audience of this addendum, if you are responsible for getting a company with at least three locations through the TISAX process.

We expect all readers to already have a good understanding of the TISAX concept and its terminology.

1.4 Structure

First, we explain whether one of our TISAX-accredited audit providers can apply the simplified group assessment to your situation. Then we point out aspects to consider when deciding whether this makes sense for your company. We present some additional requirements you need to deal with. And finally we explain how the assessment process works and where it is different from the regular process.

The estimated reading time for the document is 25-30 minutes.

1.5 How to use this document

We assume you have already read our TISAX participant handbook. If not, please do so before continuing. Understanding the content of this document is impossible without the knowledge of what the handbook explains.
You can download the TISAX participant handbook on our website at:

- [https://enx.com/tisax/tisax-en.html#registration](https://enx.com/tisax/tisax-en.html#registration)

Direct PDF download:


This document 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 addendum or is not easy to understand, please don’t hesitate to let us know. We and all future readers of this addendum will be thankful for your feedback.

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:  
[enx@enx.com](mailto:enx@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](https://en.wikipedia.org/wiki/Coordinated_Universal_Time#UTC%2B01%3A00)).

We speak English and German.
2 Introduction

**The Simplified Group Assessment in a Nutshell**

**Who?** Companies with at least three locations

**What?** A special assessment process for companies with many locations

**When?** As a preemptive step (usually before a partner asks for TISAX results)

**Where?** Focus on headquarter and a subset of all locations

**Why?** Less effort for companies with many locations and a centralised and highly developed ISMS

**How?** Deep dive at headquarter plus validation at sample locations

*Figure 1: The simplified group assessment in a nutshell*

### Is the simplified group assessment something for me?

This is the first question we will help you answer with this document. We will explain under which conditions a simplified group assessment is possible and recommended.

However, choosing the simplified group assessment is always optional. You can always stay in the regular process. You will receive TISAX labels either way and thus fulfil your partner’s request.

Next, we will present you the pros and cons of the simplified group assessment. This enables you to choose wisely between the regular process and the simplified group assessment.

Once you decided to do a simplified group assessment, you need to consider additional requirements. The additional requirements dock to the chapters in the VDA ISA document. To be prepared for a simplified group assessment, you need to fulfil all of them.

If you are confident that you fulfil all the additional requirements, you can start the TISAX process. You need to register as a TISAX participant and depending on your assessment objectives you need to register one or more scopes. With a completed registration, you can contact our TISAX-accredited audit providers and explicitly request offers for a simplified group assessment.

The main event during a simplified group assessment is the precondition check. It is an extension of the initial assessment. Its purpose is to check whether all conditions for the simplified group assessment are fulfilled.

Only if you pass the precondition check, the simplified group assessment process continues. Subsequently, so-called sample checks are conducted at a subset of all locations in the assessment scope. All remaining locations are then subject to simplified checks.
You can only pass the simplified group assessment if all checks are passed with positive results.
The publication and sharing of your assessment result is the same as for the regular process.

Now let's find out whether the simplified group assessment can be applied to your particular situation.
3 Applicability

Can the simplified group assessment process be applied to your situation? To find out, we will present the conditions in this section.

There are two main conditions:
1. Minimum number of locations in the assessment scope
2. Centralised and highly developed ISMS

Both conditions are described in detail in the following sections.

3.1 Minimum number of locations in the assessment scope

We offer the simplified group assessment for companies with many locations where running through the regular process would be unnecessarily extensive. Therefore, your company needs to have a certain number of locations before the simplified group assessment can be applied.

The general rule is that you must have at least three locations in your assessment scope. If you have less, then you need to follow the regular process.

![Figure 2: Minimum number of locations in the assessment scope](image)

3.2 Centralised and highly developed ISMS

The simplified group assessment is only possible for companies that have a centralised and highly developed ISMS:

Here’s what TISAX considers as “centralised and highly developed”:

- Your head quarter must be able to enforce all ISMS-related rules and policies at all locations in the assessment scope.
- The dependent locations must have a reliable channel back to the head quarter.
- Their feedback must match with the expectations set by the head quarter’s rules and policies.

A main characteristic of the simplified group assessment process is that the audit provider will check even more thoroughly during the assessment of your head quarter than in the regular process. The purpose is to find out whether your ISMS is sophisticated enough to warrant less intense checks at the other locations.
4 Considerations

This section presents the pros and cons of the simplified group assessment. It should help you consider all the relevant aspects and enable you to decide whether the simplified group assessment is an option for you.

Please note:
The simplified group assessment is optional. You can always decide to follow the regular process.

4.1 Pros

Reduced overall effort:
The efforts at the headquarter are higher than in the regular process. But averaged over all locations, the efforts can be significantly lower than in the regular process.

This is due to the fact that:

- sample checks are only conducted at a subset of all locations in the assessment scope and
- simplified checks are conducted at all remaining locations.

The following diagram illustrates how the simplified group assessment can reduce the overall effort. For the main location and the sample locations the effort is higher, because the audit provider assesses the central processes in depth. For the remaining locations he also assesses the central processes, but since the assessment level is lower, the overall effort per locations is lower. In the regular process on the other hand, the audit provider would have assessed all those locations with the same assessment level.

![Effort comparison diagram](image)

Figure 3: Effort comparison between the simplified group assessment (“SGA”) and the regular process (“Reg”)

You can benefit from further effort reductions like overlapping assessment scopes.
Easier to keep your assessment scope current:
It is easier to keep your assessment scope current in these cases:
1. Structural changes
2. Location changes
   a) New location
   b) New entity

It is easier to later add new locations or entities (e.g. a new company at an existing site) to your assessment scope(s) during the validity period of the original assessment. You benefit from the simpler checks for new locations. However, this only counts as an advantage if you expect a certain fluctuation in the number of locations.
For more information on when which kind of check is applied, please refer to section “8.1 Additional locations (scope extension assessment)” on page 27.

Quicker:
While the preparation may take longer, the overall time to receive assessment results for all locations can be less than in the regular process.

4.2 Cons

Higher efforts at the head quarter:
The efforts at the head quarter are higher than in the regular process. You should consider this aspect if it’s urgent for you to get TISAX-assessed. Getting a certain location TISAX-assessed is quicker in the regular process. This is a reason why most companies which choose the simplified group assessment are doing so as a pre-emptive step.

Higher level of organisation required:
The head quarter must operate with a higher level of organisation than for the regular process. The higher level is defined by the additional requirements.
For more information, please refer to Table 3: The six additional VDA ISA requirements for simplified group assessments on page 17.

More possibilities to fail:
To benefit from the simplified group assessment, you need to pass ALL checks. If you fail at any of the checks, you fall back to the regular process. Such a fall back would mean that the audit provider has to conduct regular assessments for ALL locations.

More complex planning:
The entire assessment process is more complex. Thus, your planning will be more complex.

4.3 Further considerations

It will be obvious to you by now, but for the sake of completeness: Just getting one or a few locations TISAX-assessed is much easier in the regular process.
**Break-even point for number of locations:**

We would like to give you an exact number of locations for which the simplified group assessment would most likely lower the overall efforts compared to the regular process. But due to the many factors influencing the overall effort of getting a company with many locations TISAX-assessed, we can only state that – as a very rough estimate – we consider this number to be seven. But keep in mind that when approaching TISAX in a strategic way, starting with fewer locations may still be enough to justify the initially higher overall effort.

**Starting small:**

Are you still working on establishing a centralised and highly developed ISMS? And maybe some locations are already fully managed by your centralised ISMS, but others aren’t. Then you can consider starting a simplified group assessment just for the locations that are ready for it. Thus, those locations can receive TISAX labels as early as possible. You can add the other locations one by one, as soon as they are ready. Adding locations is easier than in the regular process.

For more information on adding locations, please refer to section “8.1 Additional locations (scope extension assessment)” on page 27.

**CISO control:**

A company’s chief information security officer (CISO) may need/get more control.
4.4 Comparison with regular process

The following table roughly summarises where the simplified group assessment process is different than the regular process:

<table>
<thead>
<tr>
<th>TISAX process element</th>
<th>Simplified group assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>= No difference</td>
</tr>
<tr>
<td>Requesting offers</td>
<td>≠ Explicit request to the audit provider required</td>
</tr>
<tr>
<td>Self-assessment</td>
<td>≠ Extended (with additional requirements)</td>
</tr>
<tr>
<td>Assessment process</td>
<td>≠ Extended initial assessment (precondition check) at head quarter On average, reduced effort over all other locations</td>
</tr>
<tr>
<td>Exchange</td>
<td>= No difference</td>
</tr>
</tbody>
</table>

Table 1: Differences between the regular process and the simplified group assessment process

Figure 4: Simplified group assessment process: Only the assessment step is different than in the regular process
5 Registration

You have decided to do a simplified group assessment? Then you can start the simplified group assessment process. The process mostly follows the regular process described in the TISAX participant handbook. The differences are described this section (Registration) and the next (Assessment).

5.1 Preparation

As for the regular process, we recommend to prepare the registration. Most of our recommendations also apply to the simplified group assessment. The differences are described in the following sections.

5.1.1 Applicability check

This first step is not part of the regular process. Based on the additional requirements, you should assess internally whether you (already) fulfil the requirements. If not, you should implement (and test) any changes prior to starting the simplified group assessment.

5.1.2 Scoping

Scoping in the context of the simplified group assessment can be quite complex. We'll explain all facets in this section. We hope to enable you to find the best approach to your situation.

Generally, we recommend following these steps:

1. Create a table that contains all your locations (put all locations in the first column, one per row)
2. Add a column per assessment objective
3. For each location, mark which assessment objective it needs
4. Put all locations that need the same assessment objective in one assessment scope (column = scope)
5. Use the result to register the assessment scope(s)

The steps are the same, regardless whether you have one or more assessment objectives.
Example table:

**AO = Assessment objective**

<table>
<thead>
<tr>
<th>Location</th>
<th>AO1: Info high</th>
<th>AO2: Info very high</th>
<th>AO3: Proto high</th>
<th>AO4: Proto very high</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Example table for the scoping steps

If you have just one assessment objective or all locations have the same assessment objectives, the situation looks similar to the regular process. Yet you will benefit from the reduced efforts of the simplified group assessment because for most of your locations the assessments will be easier. And adding new locations later on is easier, too.

When you have a heterogeneous scenario where not all locations have the same assessment objective(s), the benefits of the simplified group assessment might be even bigger. At first glance, it might look counter-intuitive because having several overlapping assessment scopes might mean an unnecessary number of sample checks. But these assessment scopes are not looked at like in the regular process. Rather, a sample check at any locations can count for the other scopes as well.

For more information on the sample size, please refer to section “6.3.5 Sample size” on page 21.

### 5.1.3 Registration fee

As in the regular process, the registration fee is based on the number of locations in an assessment scope. However, in the simplified group assessment process, any location with more than one assessment objective will be part of more than one assessment scope. For such cases, you would pay the location-based registration fee as many times as a location is part of assessment scopes. As this could result in a high total registration fee, we offer additional pricing models which can reduce costs. For more information, please refer to our current price list.

You can download the price list on our website at:

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

### 5.2 Online registration process

The registration process mainly follows the steps outlined in the TISAX participant handbook. There are only differences when you register your assessment scope(s).

When you are offered to register an assessment scope, we recommend only registering one scope at this stage (even if you already know you need more than one).
We advise you to take the following steps:

- Create your head quarter as a location
- Create new assessment scope
- Add the head quarter to this assessment scope
- Continue the online registration process (invoicing information, etc.)

When you are asked to specify the scope name, we recommend the following naming pattern:

**Pattern:** SGA [Assessment objective(s) in short form]

**Examples:**
- SGA Info very high
- SGA Info high + Proto high

This allows our staff that handles your application to easily recognize your company and this scope as a candidate for a simplified group assessment. The scope name will also help your TISAX-accredited audit provider.

Once you completed the online registration process, you should follow these steps:

- Create all locations
  - Simply creating locations and not adding them to a scope has no impact on the amount of the registration fee. Some companies even add ALL their locations, even if some are not (yet) ready for TISAX.
- Create assessment scopes as needed
- Add locations to assessment scope(s)
  - The process is easier when you can select from previously created locations.

The general rule is to group locations in an assessment scope that share the same assessment objectives. Yet if you have a wide variety of assessment objectives among your locations, grouping all locations by assessment objective may make more sense. For more information on this, please refer to section “5.1.2 Scoping” on page 14.

**Please note:**
Adding many locations in the ENX portal may be a lot of clickwork. Therefore, we offer an Excel spreadsheet as an alternative data entry method. It contains columns for all the things the online registration process asks for.

This usually makes adding locations easier, especially when different individuals inside your company have to contribute data.

Please contact us to obtain the spreadsheet.

**Important note:**
If you want to discuss your simplified group assessment plans, please don’t hesitate to contact us at any stage in the process.

You are now ready to start the assessment process.
6 Assessment

6.1 VDA ISA self-assessment

The simplified group assessment requires an extended VDA ISA self-assessment. Below is the list of six additional requirements. They extend the requirements for the respective question in the VDA ISA. All additional requirements have the requirements level “MUST”. They apply to both protection levels of the criteria catalogue “Information security”.

<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
<th>Additional requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1.1 - To what extent is an Information Security Management System approved by the organization’s management and is its scope documented.</td>
<td>The ISMS in scope must be approved by an entity that has responsibility for the whole scope (i.e. all locations within the scope) and has the authority to define necessary rules and monitor their implementation.</td>
</tr>
<tr>
<td>2.</td>
<td>5.1 - To what extent is an information security policy created, published or distributed and is it reviewed at regular intervals?</td>
<td>The auditee must have specified central policies that implement all requirements of the controls of the criteria catalogues in question (i.e. VDA ISA). The policies must be published and implemented in the whole scope. The efficiency in all locations must be checked regularly through internal audits (see also 6).</td>
</tr>
<tr>
<td>3.</td>
<td>6.1 - To what extent are responsibilities for information security defined and assigned?</td>
<td>A named person having the overall responsibility for the ISMS for the whole scope must exist. This person must have the authority to monitor implementation for the whole scope and must remove all locations that do not implement appropriately from the scope. This person should be available during the precondition check.</td>
</tr>
<tr>
<td>4.</td>
<td>16.1 - To what extent are responsibilities, procedures, reporting channels and criticality levels established to ensure an effective response to information security incidents or weaknesses?</td>
<td>The auditee must have standard mechanisms that ensure that relevant security incidents are reported and recorded centrally.</td>
</tr>
<tr>
<td>5.</td>
<td>18.3 - To what extent is the ISMS reviewed by an independent third party at regular intervals or in case of significant changes?</td>
<td>The auditee must have a detailed internal audit plan and schedule that ensure that internal audits are conducted regularly and in case of major changes by an independent entity (i.e. external entities or special internal departments which are independent according to the definition of the international Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA) with appropriate competences. The person defined in 3. must be responsible for planning and steering of these internal audits. The independent entity must track findings and implementation of corrective actions. The independent entity must report to the person defined in 3. The auditee must have provided evidences clearly documenting that the whole scope is covered by the internal audit plan.</td>
</tr>
<tr>
<td>6.</td>
<td>18.4 - To what extent is the compliance of procedures and processes with policies, regulations and other relevant information security standards ensured?</td>
<td>The auditee must have highly developed efficiency checks (e.g. dedicated and appropriate information security audit responsibilities and resources) for the whole scope. These efficiency checks must include the implementation of all requirements of the controls of the criteria catalogues. The efficiency checks must be conducted and documented according to the plan described in 5.</td>
</tr>
</tbody>
</table>

Table 3: The six additional VDA ISA requirements for simplified group assessments
6 Assessment

Figure 5: Where the additional requirements dock to in the VDA ISA document

To be prepared, you must conduct the self-assessment and answer the respective question with the additional requirement in mind. Your implementation description and reference to documentation must cover the additional requirements (as if they were written in the VDA ISA).

Figure 6: The additional requirements as if they were included in the VDA ISA document

It is mandatory to have a self-assessment for every location. However, this “self-assessment” must not necessarily be a “VDA ISA self-assessment” (in its Excel manifestation). With appropriate mapping, you can use the information from your ISMS to produce an acceptable self-assessment artefact.

You have to ensure the following:

- The answers to all questions (including evidences) in the VDA ISA must be centrally available.
- The answers must be available for all locations in the assessment scope.
- You must provide an easy method for mapping your answers to the questions in the VDA ISA.

Please discuss this point with your audit provider. He has to confirm that your approach is acceptable.

6.2 Requesting offers from TISAX-accredited audit providers

When you request offers from our TISAX-accredited audit providers, you must explicitly mention the fact that you intend to do a simplified group assessment. The audit provider is not obliged to point out that this option exists or may be applicable to your situation.
6.3 Assessment process

6.3.1 Location classes and check types

In the regular process, every location is subject to the same intensity, assessment methodologies, etc. (of course depending on the assessment objective). In the simplified group assessment process there are now three different classes of locations which are each subject to a different type of “check”.

![Figure 7: The location classes](image)

<table>
<thead>
<tr>
<th>Location class</th>
<th>Check type</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main location (head quarter)</td>
<td>Precondition check</td>
<td>PCC</td>
</tr>
<tr>
<td>Sample location</td>
<td>Sample check</td>
<td>SAC</td>
</tr>
<tr>
<td>Remaining location</td>
<td>Simplified check</td>
<td>SIC</td>
</tr>
</tbody>
</table>

*Table 4: Location classes and check types*

![Figure 8: The locations classes and check types](image)

All locations must be part of the assessment scope, regardless of their class.
Each check type is different in the following ways:

<table>
<thead>
<tr>
<th>Check type</th>
<th>Additional requirements</th>
<th>Assessment level</th>
<th>Locality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precondition check</td>
<td>Yes</td>
<td>Always AL 3</td>
<td>Always “On site”</td>
</tr>
<tr>
<td>Sample check</td>
<td>Yes</td>
<td>AL 3 or AL 2</td>
<td>“On site” or “Remote”</td>
</tr>
<tr>
<td>Simplified check</td>
<td>Yes</td>
<td>AL 2 or AL 1</td>
<td>“On site” or “Remote”</td>
</tr>
</tbody>
</table>

*Table 5: Check type differences*

**Additional requirements:**
The additional requirements cover the central processes. They vary slightly over the location classes. At the main location, the audit provider focuses on the head quarter’s role as the hub of the ISMS. For the other locations, the audit provider focuses on how predictably and reliably the spokes interface with the hub.

**Assessment level:**
For the main location, the assessment level is always AL 3. For sample locations, the assessment level can be either AL 3 or AL 2. For the remaining locations, the assessment level can be either AL 2 or AL 1.

**Locality:**
The precondition check is always conducted “on site”. For the other check types, the locality is derived from the requirements that come with the respective assessment objective.

Example: For both prototype assessment objectives, the locality must be “on site”.

### 6.3.2 Precondition check

The assessment is the same as in the regular process. But it is extended by the precondition check.

The precondition check is conducted at the location from which the information security is managed (usually the company’s head quarter).

With the precondition check the audit provider checks whether the additional requirements are fulfilled.

It is always conducted on site and with assessment level 3 (AL 3).

The precondition check has the purpose to create a detailed expectation of how the ISMS works across all locations. If all requirements are met, the audit provider will have a clear view on what to expect once he continues with the sample checks.

During the precondition check the audit provider checks whether the answers to the VDA ISA questions for all locations in the assessment scope are available.

If the precondition check fails, the simplified group assessment process is aborted.

### 6.3.3 Sample checks

A successfully passed precondition check is a mandatory condition for the sample checks.

The sample check is conducted at the sample locations (a subset of all locations in an assessment scope).

The purpose of the sample checks is to verify that the observations at every sample location match with the expectations set during the precondition check.
The audit provider first conducts a regular assessment (as required by the assessment objective(s)). Then he verifies that the central processes are correctly implemented. For more information on the number of sample checks, please refer to section “6.3.5 Sample size” on page 21. For more information on the selection of sample locations, please refer to section “6.3.6 Sample selection” on page 22.

6.3.4 Simplified checks

All sample checks must be successfully passed before the process can continue with the simplified checks of the remaining locations.

The audit provider will usually check all remaining locations with a lower assessment level than applied to the sample checks.

For more information, please refer to section “6.3.7 Assessment levels” on page 22.

6.3.5 Sample size

The audit provider must conduct sample checks at a defined minimum number of sample locations.

The minimum number of locations in the sample depends on the total number of locations in your assessment scope. The minimum number of sample locations always starts at two.

The minimum number of locations in the sample is calculated based on a formal equation. However, we start with a version in plain English:

1. Take the total number of locations in your assessment scope \( (\text{No}_{\text{location}}) \).
2. Is your total number of locations:
   a) less than or equal to 10?
      Then your minimum number of sample locations is 2.
   b) greater than 10, but less than or equal to 50?
      Then subtract 10, multiply with 0.1, add 2.
   c) greater than 50?
      Then subtract 50, multiply with 0.05, add 6.
3. Take the result and round up to get the minimum number of sample locations \( (\text{No}_{\text{samples}}) \).

Examples:

<table>
<thead>
<tr>
<th>Total number of locations</th>
<th>Minimum sample size</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>42</td>
<td>6 (rounded up from 5.2)</td>
</tr>
<tr>
<td>128</td>
<td>10 (rounded up from 9.9)</td>
</tr>
</tbody>
</table>

*Table 6: Examples for sample sizes*
Here's a visual approach:

Figure 9: The sample size diagram

And this is the formal equation:

\[
No_{\text{sample}}(No_{\text{locations}}) = \begin{cases} 
2, & No_{\text{locations}} \leq 10 \\
[0.1(No_{\text{locations}} - 10) + 2], & No_{\text{locations}} \leq 50 \\
[0.05(No_{\text{locations}} - 50) + 6], & No_{\text{locations}} > 50 
\end{cases}
\]

Equation 1: Minimum number of sample locations

The result is always rounded UP.

Important note:
The number of locations in the sample can be higher than the calculated minimum number. For more information, please refer to the next section.

6.3.6 Sample selection

The audit provider:
- selects the sample locations from the total number of locations in the assessment scope.
- selects at least as many locations as calculated for the sample size.
- can decide to conduct sample checks at more locations than indicated by sample size.
- does the selection based on the probability of non-conformities and the possible impact of non-conformities. All this is based on the audit provider’s professional judgement.
- documents his justification for the selection of the subset.

6.3.7 Assessment levels

The assessment levels reflect a tiered approach for gaining confidence in whether the requirements are fulfilled.
Generally:

In an assessment with assessment level 3, the audit provider obtains his own impression. He’s really aiming to understand and observe how the requirements are fulfilled. He does not solely rely on documentation or statements.

In an assessment with assessment level 2, the audit provider (selectively) compares what the ISMS suggests he would observe against the real situation at that location.

In the context of the simplified group assessment:

The main location is always assessed in an assessment with AL 3. The audit provider aims to get a comprehensive idea of how the ISMS works. He focusses especially on the central processes and how they take effect on the dependent locations. The audit provider builds up a detailed picture of what he expects to observe at the dependent locations.

The sample locations are then assessed with the focus on verifying the picture that emerged during the precondition check at the main location. The sample checks are conducted either with AL 3 or AL2.

Successful assessments of the main location and the sample locations warrant that the remaining locations are assessment with a lower assessment level. Thus, the simplified checks at the remaining locations are either conducted with AL 2 or AL 1.

The following table shows the assessment level and the assessment locality for each location class:

<table>
<thead>
<tr>
<th>No.</th>
<th>Assessment objective</th>
<th>Main location</th>
<th>Sample locations</th>
<th>Remaining locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Information with high protection level</td>
<td>AL 3</td>
<td>On site</td>
<td>AL 2</td>
</tr>
<tr>
<td>2.</td>
<td>Information with very high protection level</td>
<td>AL 3</td>
<td>On site</td>
<td>AL 3</td>
</tr>
<tr>
<td>3.</td>
<td>Connection to 3rd parties with high protection level</td>
<td>AL 3*</td>
<td>On site*</td>
<td>AL 3*</td>
</tr>
<tr>
<td>4.</td>
<td>Connection to 3rd parties with very high protection level</td>
<td>AL 3</td>
<td>On site</td>
<td>AL 3</td>
</tr>
<tr>
<td>5.</td>
<td>Handling of prototypes with high protection level</td>
<td>AL 3*</td>
<td>On site*</td>
<td>AL 3*</td>
</tr>
<tr>
<td>6.</td>
<td>Handling of prototypes with very high protection level</td>
<td>AL 3</td>
<td>On site</td>
<td>AL 3</td>
</tr>
<tr>
<td>7.</td>
<td>Data protection according to German §11 BDSG (“Auftragsdatenverarbeitung”)</td>
<td>AL 3</td>
<td>On site</td>
<td>AL 2</td>
</tr>
<tr>
<td>8.</td>
<td>Data protection with special categories of personal data</td>
<td>AL 3</td>
<td>On site</td>
<td>AL 3</td>
</tr>
</tbody>
</table>

Table 7: Assessment level and locality for each location class
Please note:
About the two assessment objectives marked with an asterisk (*):
Because these two assessment objectives mandate on-site assessments, the simplified group assessment may not make much sense in a scenario where these are the only assessment objectives. There wouldn't be a difference in efforts compared to the regular process. However, in a more heterogeneous scenario it is possible to have these assessment objectives and it may still make sense.

Please note:
The activation list can have an effect on the locality.
The assessment objectives “Con” and “Proto” mandate “on site” anyway. But for the assessment objectives “Info” and “Data”, the activation list can require “on site” assessments (for AL 2) as well.

Please note:
Some locations can face “split AL” situations.
A “split AL” situation means a location with dependent assessment objectives can be subject to checks for one assessment objective with AL 1 and to checks for another assessment objective with AL 2. Assessment objectives with dependencies (e.g. “Info” included in “Proto”) and a general “on site” requirement (currently “Con” and “Proto”) can cause “split AL” situations.
Example:
The assessment objective is “Proto high”. This includes the assessment objective “Info high”. For “Info high”, the audit provider must conduct the simplified check with AL 1. However, “Proto high” mandates the audit provider has to conduct the simplified check with AL 2 and “on site”. In such a situation, the audit provider will focus on the “Proto” requirements in an AL 2 on-site check. He will also focus on any “Info” requirements that are closely linked to the “Proto” requirements. He will check all other “Info” requirements as in a typical AL 1 check.

Important note:
It is essential to understand that assessment level and assessment locality don't have a fixed 1:1 relationship – even it in many cases it looks like one.
An AL 3 assessment will always be “on site”. But for the other locations, an AL 2 assessment can be “remote” (e.g. for assessment objective “Info high”) or it can be “on site” (e.g. for assessment objective “Proto high”).
In some cases, the localities are mandated by the assessment objectives and whether the location is in a country that is listed in the activation list.

6.3.8 Conformity

The audit provider focuses on the fulfilment of the additional requirements. The find of a major non-conformity automatically implies that the additional requirements for the simplified group assessment are not fulfilled. Therefore, if the audit provider finds new major non-conformities that are not known to and not managed by the ISMS, he must abort the simplified group assessment. He won't abort the process, if the major non-conformity is known to and managed by the ISMS.
A new simplified group assessment is only possible, if you can prove structural changes that prevent major non-conformities at all locations.
Important note:
The abortion of the process when the audit provider finds a new major non-conformity is an essential difference to the regular process. If the audit provider finds a major non-conformity in the regular process, you simply mitigate and resolve it (as documented in a corrective action plan) and request a new follow-up assessment. You don’t have this option in the simplified group assessment.

6.3.9 Process duration

It is impossible for us to give you a reliable estimate regarding the process duration. It depends on too many factors. If you have to get 20 identical data centres TISAX-assessed, the process is much faster than for an automotive tier-1 supplier with a wide variety of businesses.

Factors you need to consider are:
- Number of locations
- Homogeneity of the locations
- Quality and structure of the internal ISMS documentation at the head quarter (central availability of information about all locations)

6.3.10 TISAX report

The TISAX report is the only place where you will see that the audit provider conducted a simplified group assessment. Any publication or sharing permission granted via the ENX portal does not give this information.
7 Exchange

There is no difference in the process to publish and share your assessment result compared to the regular process.
8 Lifecycle management

8.1 Additional locations (scope extension assessment)

You can add one or more locations to your existing assessment scope. The new locations must be part of the central ISMS.

If you add new locations to your assessment scope, the required minimum number of sample locations may change. If the sample size changes, your audit provider has to repeat the sample selection step (“6.3.6 Sample selection” on page 22). If the audit provider must add sample locations, he can select them from the existing locations and/or the new locations.

If new locations aren't selected as sample locations, the audit provider will conduct simplified checks instead of sample checks.

If the sample size doesn't change even with the new locations, the audit provider will by default also conduct simplified checks. However, if the audit provider expects any risks regarding the new locations, he has to conduct sample checks.

![Decision tree for determining the check type for new locations](image_url)

*Figure 10: Decision tree for determining the check type for new locations*

When the checks are successfully passed, the audit provider issues an updated TISAX report.

The updated TISAX report contains:

- Information about the new locations
- Information about additional sample checks, if applicable
- Justification for the sample selection, if applicable
The audit provider notifies us about the new locations and we update the assessment scope information in the ENX portal accordingly.

The validity period of the assessment result and the corresponding TISAX labels does not change if you add new locations.

Only the audit provider that did the original simplified group assessment can add new locations.

Please note:
We recommend creating the new locations in the ENX portal as your first step. The second step is to then request the scope extension assessment from your audit provider.

Important note:
If you add a new location and the audit provider finds a major non-conformity (that is not already managed by the ISMS), the entire assessment scope is at risk of losing its TISAX labels. This won't happen for minor findings. But if the non-conformity suggests major risks that are unmanaged by the ISMS, the audit provider can't justify that you can keep your TISAX labels.

8.2 Removing locations

You are obliged by the “TISAX Participation General Terms and Conditions” to notify us, when something changed in a way that the requirements aren't fulfilled anymore.

Examples for such changes:

- a location stopped following the central processes
- a location is no longer under the full control of the central ISMS
- a location was sold to another company
- a location declared bankruptcy

We will remove the location(s) from the assessment scope. The audit provider won't issue an updated TISAX report.