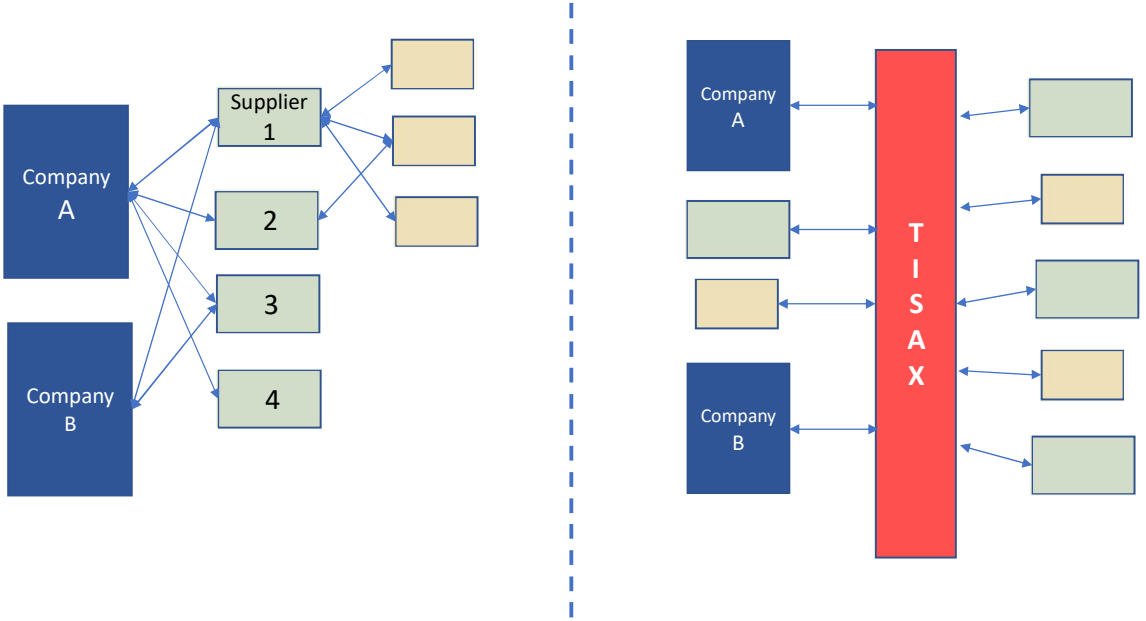
Jos Waegemaekers

September 2018

Tisax: intro

- **T**rusted **I**nformation **S**ecurity **A**ssessment **E**xchange.
- Active in automotive industry, area Information Security Management
- No new specification, it is using VDA – ISA norm; VDA-ISA based upon ISO2700x
- Collecting proof that your ISM is according to specification
- Providing infrastructure to share this with partners

WoW old vs new



TISAX process

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

Figure 1: TISAX process overview

- STEP 1: define scope, provide information to TISAX (and pay a fee…)
- Step 2: Assessment (audit) by TISAX-accredited audit provider
- Step 3: partner controlled exchange of results

Terminology

- Objective vs label:

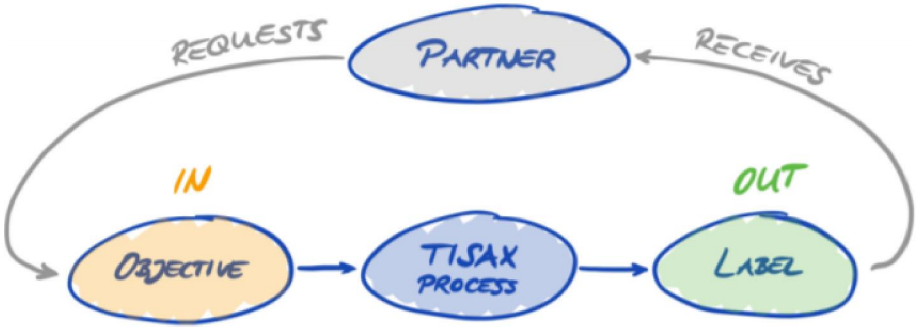


Figure 9: Assessment objectives and TISAX labels

VDA terminology: Criteria Catalogue

Terminology

- 8 Assessments objectives
- In latest (4.0.4, june 2018) VDA checklist criteria catalogue “Data” removed
- Assessment levels (AL1: internal, AL2/3: TISAX involved)

The current TISAX assessment objectives are:

No.	Assessment objective	Abbreviation
1.	Information with high protection level	Info high
2.	Information with very high protection level	Info very high
3.	Connection to 3rd parties with high protection level	Con high
4.	Connection to 3rd parties with very high protection level	Con very high
5.	Handling of prototypes with high protection level	Proto high
6.	Handling of prototypes with very high protection level	Proto very high
7.	Data protection according to German §11 BDSG (“Auftragsdatenverarbeitung”)	Data
8.	Data protection with special categories of personal data Special categories according to German §3 section (9) BDSG (“Besondere Arten”), Data Protection according to German §11 BDSG (“Auftragsdatenverarbeitung”)	Special data

Table 2: The current TISAX assessment objectives

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[16]	In person, on site
On-site inspection	No	Depends[17]	Yes

Table 6: Applicability of assessment methods to different assessment levels

Step 2: assessment process

TISAX accredited Audit providers:

- Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft
- KPMG AG Wirtschaftsprüfungsgesellschaft
- operational services GmbH & Co. KG
- PricewaterhouseCoopers (PERSICON cert GmbH)
- TÜV Rheinland i-sec GmbH
- Coming soon: DEKRA

Step 2: assessment process

- Audited along VDA – ISA checklist
- Standard way of working on assessment: conform / minor / major non-conformity
- Standardised reporting
- Once conform, TISAX label released, valid for 3 years.
- With minor, release of temporary label possible, valid for max 9 months, no renewal.

Step 3: exchange results

- Multiple sharing levels
- Sharing levels controlled by owner:
  1. Generic (visible to all participants): default no sharing, recommended A+labels, max B+labels
  2. Tailored for specific partner: up to E+labels

	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 11: Main sections of the TISAX report and the sharing levels on the exchange platform

TISAX: summary

- Added value: one audit result valid for multiple customers
- Limitation:
  - customer has to be partner of TISAX also
  - External auditor only from few institutes
- Strong focus on VDA ISA
- the VDA has recommended its members to bring their information protection into line with the international standard ISO 2700x
- however, VDA not straightforward covering full ISO2700x
- Looks like more for European automotive industry.