

bsi.

● Introducing TISAX<sup>®</sup>:  
trusted information security for  
the automotive sector

**TISAX<sup>®</sup>**



- What is TISAX and its benefits?
- How TISAX builds on other information security standards (ISO/IEC 27001)
- Assessment levels, objectives, maturity and results
- Steps to obtaining TISAX labels

# ● Trusted information security



Customer

Can't just "believe" you

How to ensure Supplier / partner keep Information properly?

What is security standards?

Supplier / partner

Implement according to Security standards

Proof meet Security standards

Customer

Automotive way:

- Set specific requirement
- Require to proof
- All customers is required to assessment

## ● What is TISAX?

TISAX stands for Trusted Information Security Assessment Exchange and is an assessment and exchange mechanism for information security throughout the automotive supply chain.

TISAX enables mutual acceptance of information security assessments between suppliers and partners in the automotive industry.

It was developed by VDA in collaboration with ENX, who now operate the TISAX program for VDA.

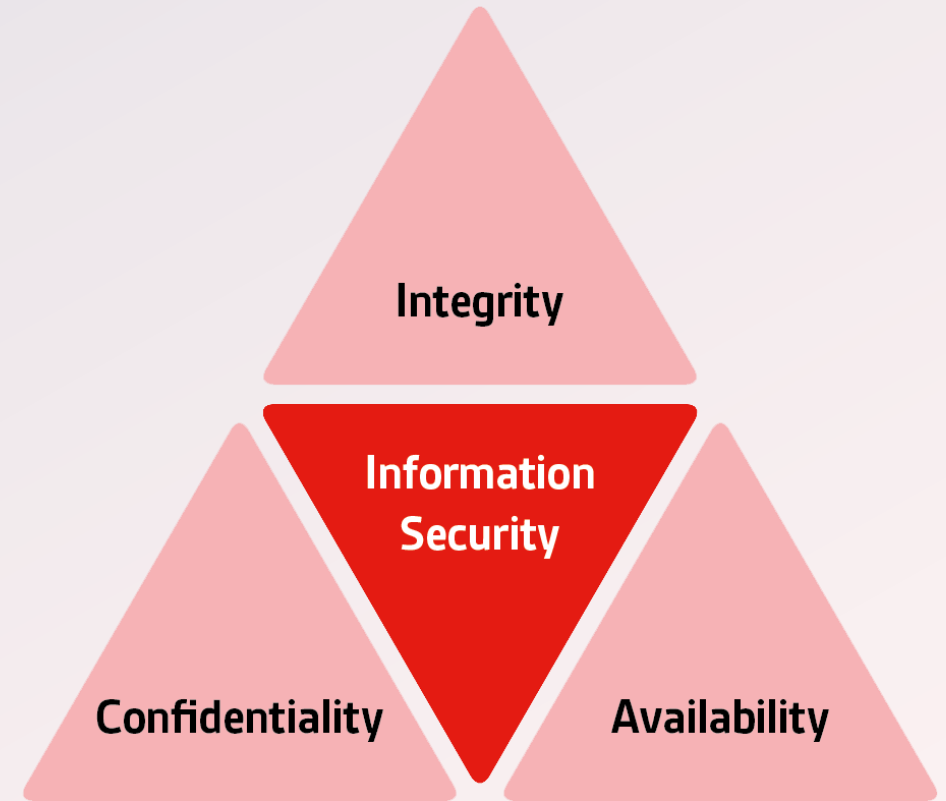


# ● Why TISAX?

Increasing industry on information and cyber security as more connected technology is adopted, large amounts of confidential and sensitive information is being exchanged.

Mandated by OEM's, including BMW, Mercedes Benz and VW. More expected to follow.

Information needs to be protected from theft, manipulation and loss.



The Pyramid of Information Security

# ● The benefits of TISAX



Standardizes automotive-specific requirements for information security



Business development opportunities thanks to industry-wide recognition



Avoids duplication of assessments and allows common recognition of results



Facilitates renewal of existing supplier contracts



Provides efficiencies for manufacturers and suppliers





Inspires confidence and trust across the automotive supply chain

## ● What's the relationship between TISAX and IATF 16949?

IATF 16949 is Quality Management system include customer specific requirement

The Verband Der Automobilindustrie (VDA) – members including BMW, Volkswagen Audi Group and Daimler – has developed the Trusted Information Security Assessment Exchange (TISAX) label.

The TISAX label is recommended by the VDA and it is mandatory to do business with certain VDA members.

IATF 16949	TISAX
	
Quality Management System	Information Security Management System
IATF Certificate	TISAX Label
No Exchange report	Exchange report

# ● What's the relationship between TISAX and ISO/IEC 27001?

TISAX assessments use the VDA ISA requirements catalogue, which refers to the information security controls of ISO/IEC 27001 in Annex A.

The VDA ISA catalogue comprises the key aspects and criteria of ISO/IEC 27001 and additional criteria, classified in three domains:

- Information Security Assessment - based on ISO/IEC 27001 Annex A
- Prototype protection requirements
- Data protection (with reference to Article 28 of GDPR)



## ● What's the relationship between TISAX and ISO/IEC 27001?

ISO/IEC 27001 focuses on the organization's own information security

TISAX emphasizes the security of third-party information within the organization's ISMS.

Domain	# controls
Information Security, based on ISO 27001 Annex a	41 controls
Prototype Protection	22 controls
Data Protection	4 controls

# ● About standards

- Assessment levels,
- Objectives,
- Maturity,
- Results

## Information Security Assessment



Verband der  
Automobilindustrie

VDA ISA provides the basis for

- a self-assessment to determine the state of information security in an organization (e.g. company)
- audits performed by internal departments (e.g. Internal Audit, Information Security)
- a review in accordance with TISAX (Trusted Information Security Assessment Exchange, <http://enx.com/tisax/>)

VDA ISA consists of several tabs, the content and function of which are explained in the tab "Definitions". The corresponding actual requirements can be found in the tabs "Information Security", "Data Protection" and "Prototype Protection".

For Version 5, VDA ISA has been restructured with the requirements no longer presented in lines but in columns. Additionally, new numbering has been introduced and topics have been combined. The numbering of ISA 4 has been retained in a separate column for easier finding of control questions according to the previous structure or to facilitate rearrangement.

**We recommend to gain an overview of the individual ISA tabs by using the "Definitions" tab. Then, commence with the "Information Security" tab.**

ENX WG ISA and the Working Group Information Security of the VDA wish you every success.

Publisher: VERBAND DER AUTOMOBILINDUSTRIE e. V. (VDA, German Association of the Automotive Industry); Behrenstr. 35; 10117 Berlin; [www.vda.de](http://www.vda.de)

© 2022 Verband der Automobilindustrie e.V., Berlin

# ● Assessment levels

The Assessment levels define the method of valuation.

- AL1: Self-assessment by the auditee. Assessment of existing self-declaration of the auditee
- AL2: Plausibility check of self-assessment restricted to evaluation of evidences and an expert interview.
- AL3: Full assessment including evaluation of evidence, on-site inspection and expert interviews.

# ● Assessment objectives and levels

No.	TISAX Assessment Objective	AL	ISA criteria catalogue
1	Information with high protection needs	AL 2	Information security
2	Information with very high protection needs	AL 3	Information security
3	Protection of prototype parts and components	AL 3	Prototype protection
4	Protection of prototype vehicles	AL 3	Prototype protection
5	Handling of test vehicles	AL 3	Prototype protection
6	Protection of prototypes during events and film or photo shootings	AL 3	Prototype protection
7	Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	AL 2	Data protection
8	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	Data protection

# ● Maturity levels

TISAX uses maturity levels as a measurement for the “maturity” of the overall ISMS, or parts of it:

Level 0: Incomplete

Level 1: Performed

Level 2: Managed

Level 3: Established

Level 4: Predictable

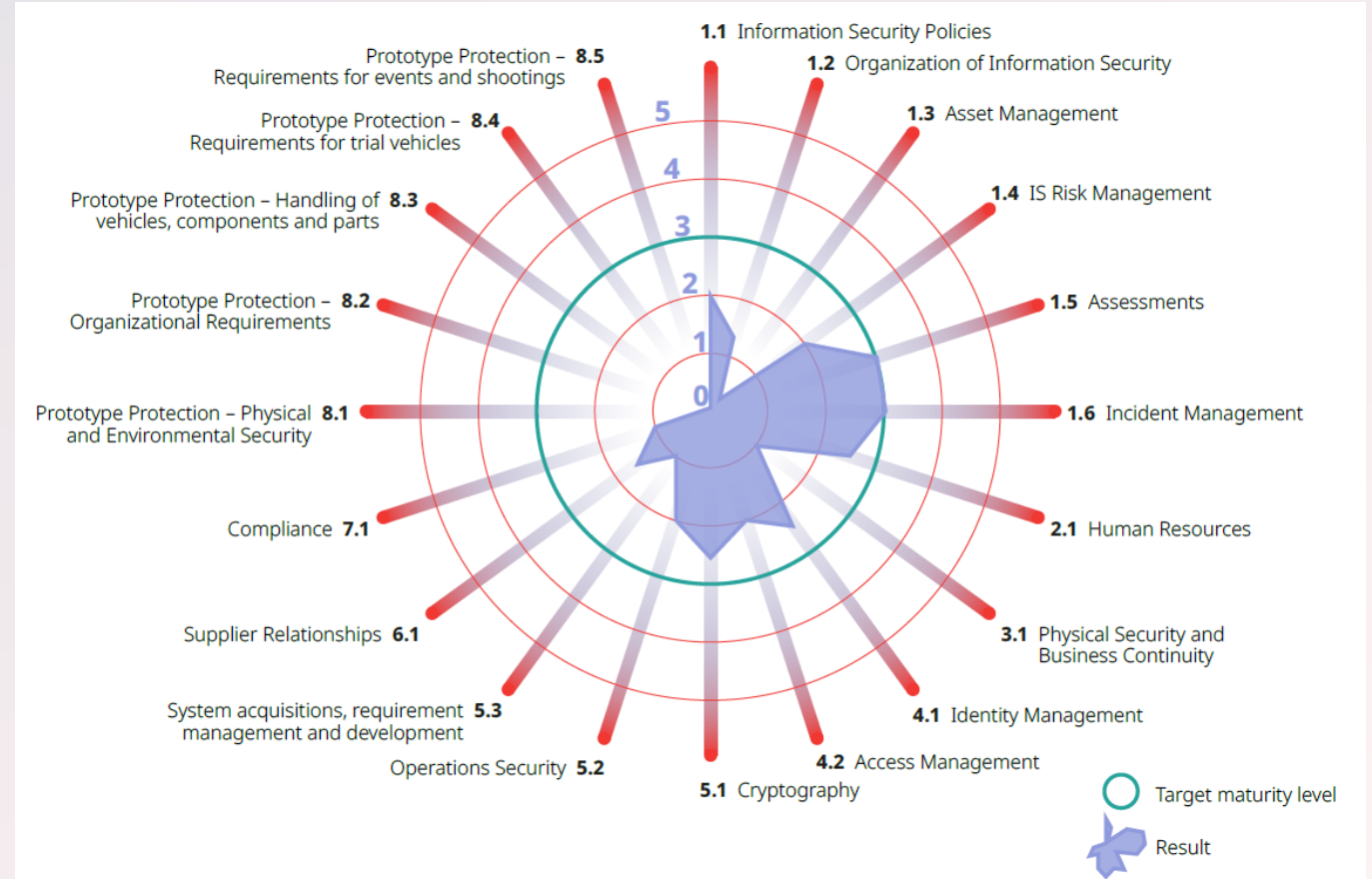
Level 5: Optimizing

# ● Assessment results and labels exchange

Assessment is performed against target maturity levels and the results are displayed as a spider diagram.

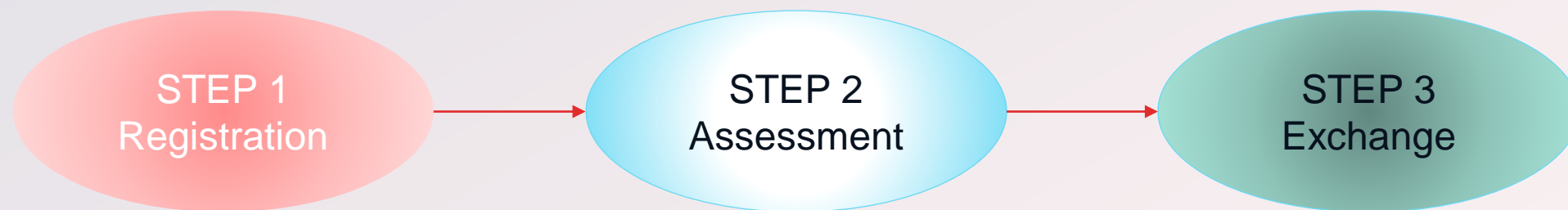
Assessment results are provided as TISAX labels on the ENX portal.

TISAX labels can then be exchanged with other registered participants in the ENX Portal.

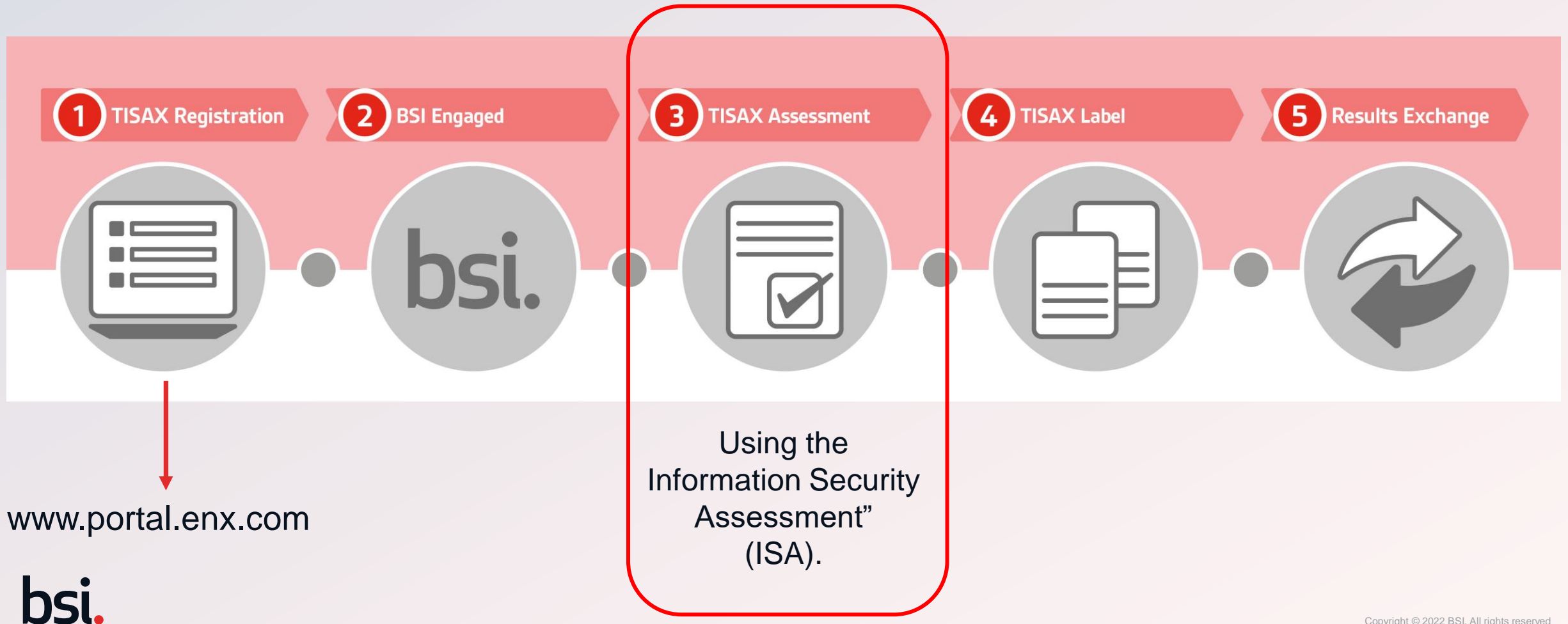


# ● Steps to obtaining TISAX labels

**Starting point:** one of your partners requesting that you prove a defined level of security management according to the requirements of the “Information Security Assessment” (ISA).

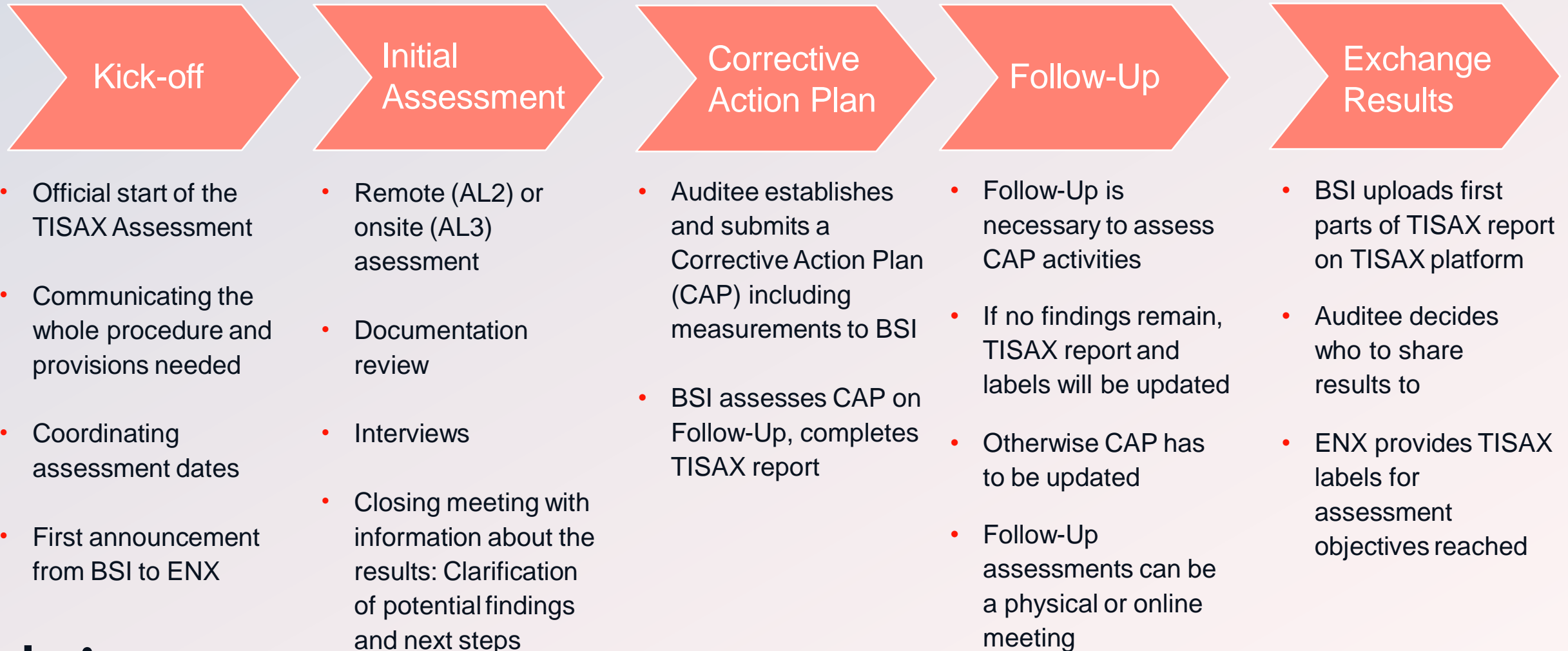


# ● The TISAX process – how to obtain the label





# ● The assessment process



A statistic, BSI issued 30 TISAX labels in 2022 in 12 different countries, (across the globe Brazil – China).



By Royal Charter



Country	Ratio
Australia	3%
Austria	3%
Canada	3%
China	3%
Germany	50%
Japan	7%
Mexico	3%
Poland	3%
Portugal	3%
Spain	3%
Switzerland	3%
The Netherlands	3%
United Kingdom	7%
USA	3%

# ● Training

We'll train you on how to implement and audit TISAX, so you're confident and ready to obtain your TISAX labels.

- Introduction course, 1 day
- Implementation course, 2 days
- Internal auditor course, 2 days



## ● Next steps

1. Download the BSI Guide to TISAX (in the handouts)
2. Register as a TISAX Participant on the ENX Portal at [enx.com](https://enx.com)
3. Determine your assessment level and objectives
4. Obtain the Scope Excerpt and share it with BSI – this is essential for assessment planning and quotation
5. Contact BSI to book your TISAX assessment and training





- **Contact us**



[www.bsigroup.com/th-TH/](http://www.bsigroup.com/th-TH/)



BSI Thailand



@bsithailand