● Webinar

# TISAX

การเตรียมความพร้อมและเข้าใจมาตรฐาน

ด้านความปลอดภัยสารสนเทศ

ในอุตสาหกรรมยานยนต์

bsi. AC INFOTEC 20th ANNIVERSARY

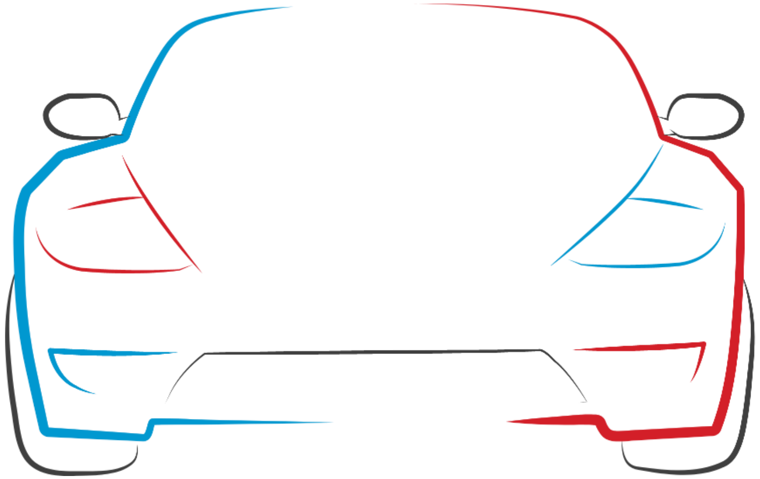
# Agenda

## Implementation part

1. What's TISAX? and Why TISAX?
2. The TISAX process and Scope of TISAX
3. TISAX requirements
4. TISAX implementation roadmap
5. Key takeaways

## Audit part

1. Why is TISAX certified?
2. TISAX assessment level
3. TISAX assessment process
4. TISAX certification maintenance program
5. Key takeaways



## Implementation part

# What's TISAX? and Why TISAX?

# What's TISAX? and Why TISAX?

**TISAX** stands for Trusted Information Security Assessment Exchange
TISAX is an assessment and exchange mechanism for the information security of enterprises and allows recognition of assessment results among the participants.

The TISAX label confirms that a company's information security management system complies with defined security levels and allows sharing of assessment results across a designated platform.

TISAX developed by VDA in collaboration with ENX, who now operate the TISAX program for VDA.
It consists of many controls derived from Annex A of ISO 27001 plus controls for the special automotive sections: Prototype Protection, Involvement of Third Parties and Data Protection.
For each control a maturity level (na, 0 - 5) needs to be specified.

# What's TISAX? and Why TISAX?

According to the standards of the automotive industry, organizations in the sector can meet the requirements of maintaining information security.

In the automotive sector, partners confidence in the information security in place for organization data.

In the automotive sector, partners belief in the safety measures of information pertaining to an individual.

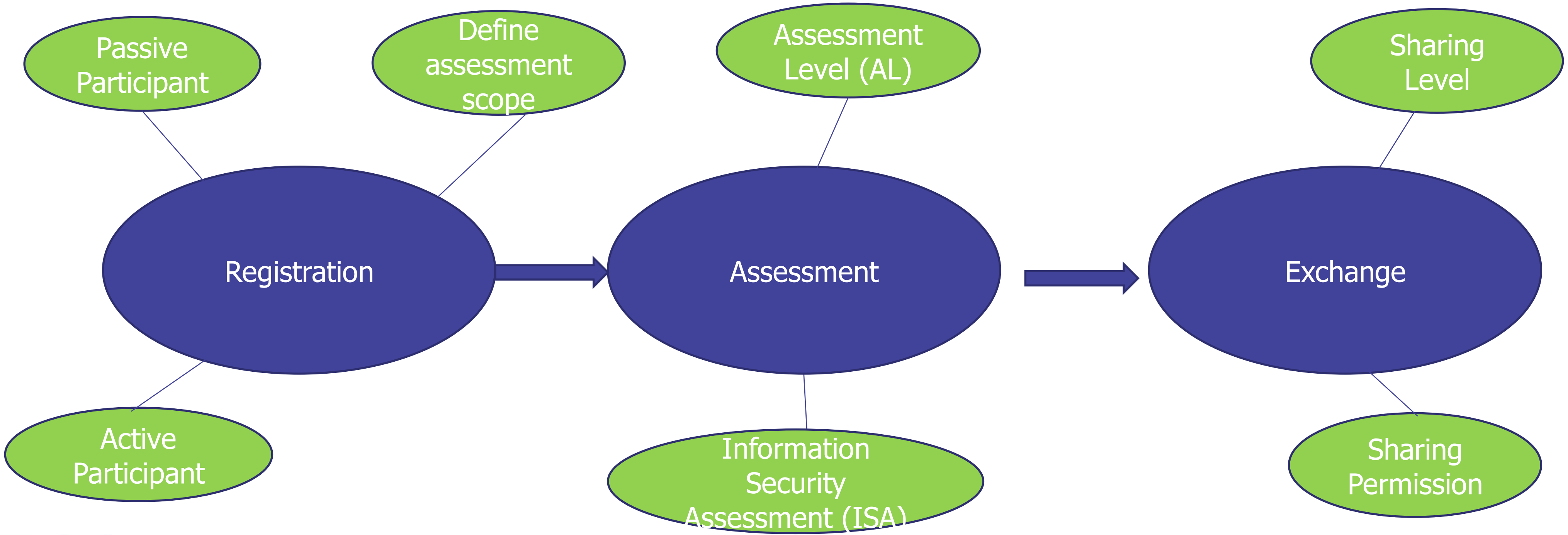
Suppliers in the automotive industry's supply chain can put security measures in place to safeguard company information and protect customer information.

## Implementation part

# The TISAX process and Scope of TISAX

# The TISAX process

1. Register TISAX Participant
2. Self Assessment and GAP Closing
3. TISAX Assessment
4. Receive TISAX Label
5. Exchange TISAX Label with other partner/participant



# Scope of TISAX

## 1. Standard scope

Receive TISAX Label

Recommend

**The TISAX scope** defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.

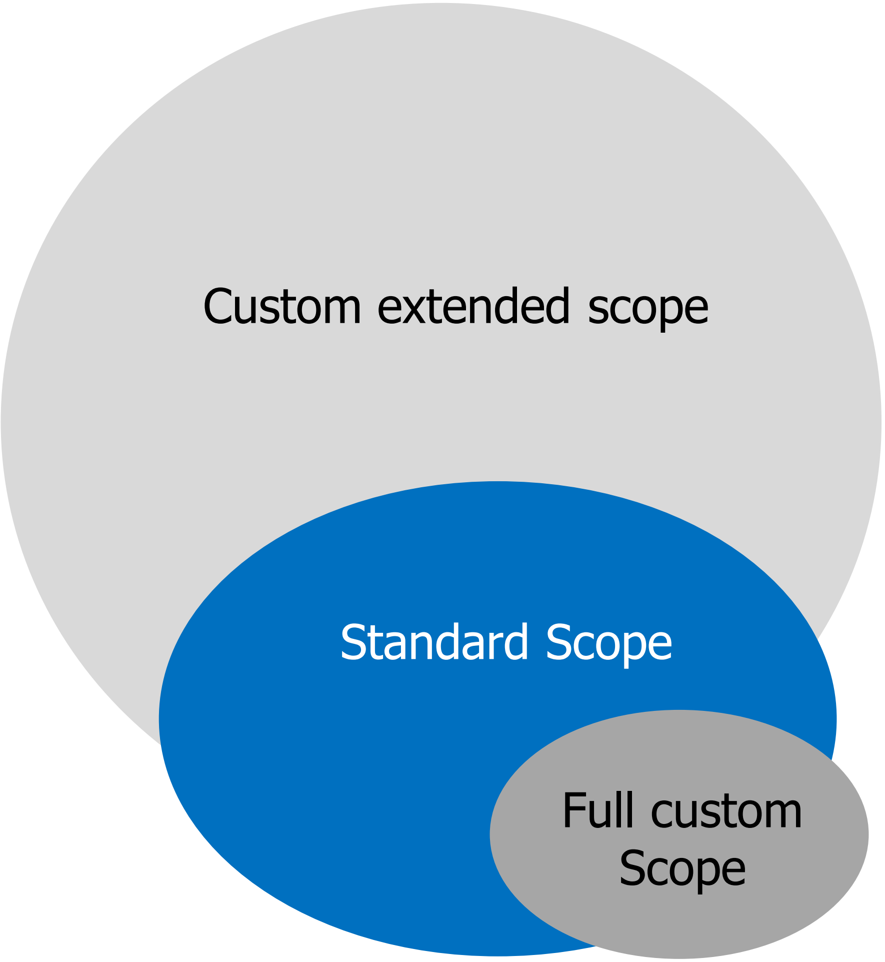
The assessment is conducted at least in the highest assessment level listed in any of the listed assessment objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

## 2. Custom scope

- Custom extended scope — Receive TISAX Label

  Extend from Standard Scope

- Full custom scope — Not Receive TISAX Label



# Implementation part

## TISAX Requirements

# TISAX requirements

## Related Document

- TISAX Participant Handbook

  TISAX Participant Handbook published by ENX Association
  Current Version: 2.6
  Date: 28-08-2023

- VDA ISA 5.1

  Information Security Assessment questionnaire published by the VDA
  Current Version: 5.1
  Date: 02-05-2022

Other related document: https://portal.enx.com/en-US/TISAX/downloads/

# TISAX requirements

## VDA ISA5.1 Structure

VDA ISA consist of security control from ISO 27001 plus controls for the special automotive sections: Prototype Protection, Involvement of Third Parties and Data Protection.

### ISO 27001 Structure including

Management system requirement : Clause 4 – 10
Security Controls: 14 Domains from A.5 – A.18

### VDA ISA5 Structure including

Chapter of control question : Chapter 1-8

# TISAX requirements

## Information Security

Specific Requirements to be respected within the organization to protect Automotive related progects/products from TISAX/ENX Stakeholders.

## Prototype Protection

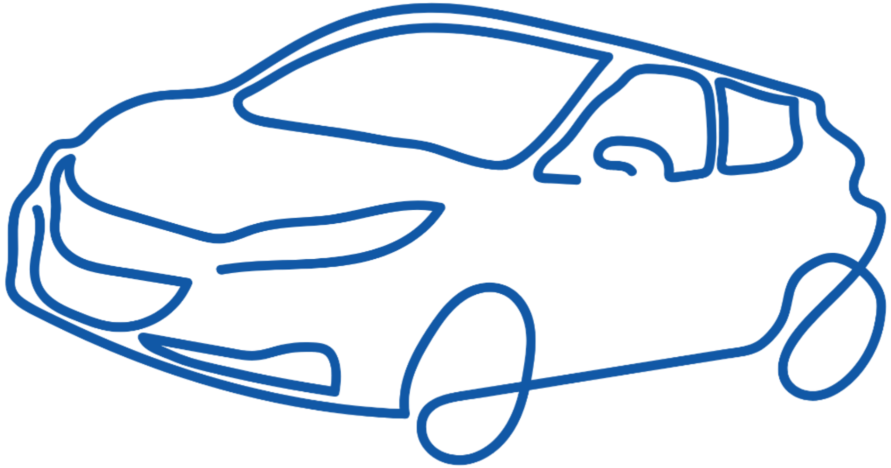
Prototype protection includes vehicles, components and parts which are classified as requiring protection but have not yet been presented to the public and/or published in adequate form by the OEM.
The commissioning department of the OEM is responsible for classifying the protection need of vehicles, components and parts. The minimum requirements for prototype protection are to be applied for protection classes High and Very high according to ISA.

## Data Protection

Data protection is to be edited additionally in case of processing within the meaning of Art. 28 of the EU General Data Protection Regulation and contains controls requiring merely yes/no answers.

# TISAX requirements: Information Security

1. IS Policies and Organization
   - 1.1 Information Security Policies
   - 1.2 Organization of Information Security
   - 1.3 Asset Management
   - 1.4 IS Risk Management
   - 1.5 Assessments
   - 1.6 Incident Management
2. Human Resources
3. Physical Security and Business Continuity



# TISAX requirements: Information Security

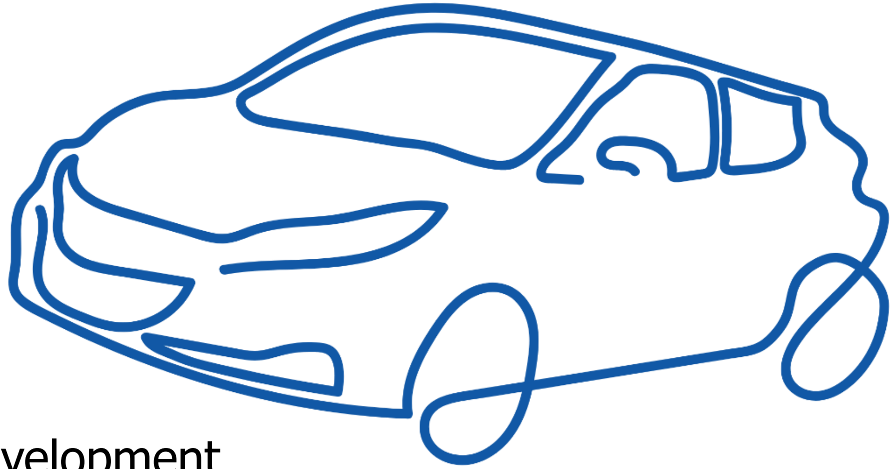
4. Identity and Access Management

    4.1 Identity Management
    4.2 Access Management

5. IT Security / Cyber Security

    5.1 Cryptography
    5.2 Operations Security
    5.3 System acquisitions, requirement management and development

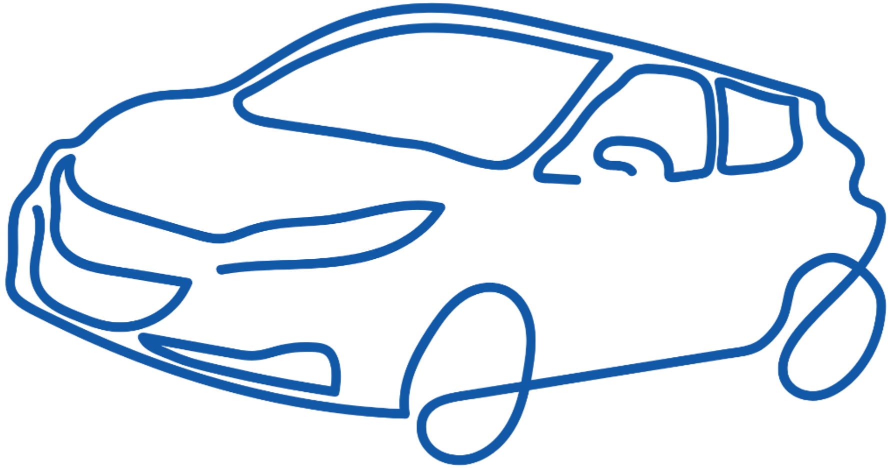
6. Supplier Relationships
7. Compliance



# TISAX requirements: Prototype Protection

8. Prototype Protection

   8.1 Physical and Environmental Security
   8.2 Organizational Requirements
   8.3 Handling of vehicles, components and parts
   8.4 Requirements for trial vehicles
   8.5 Requirements for events and shootings



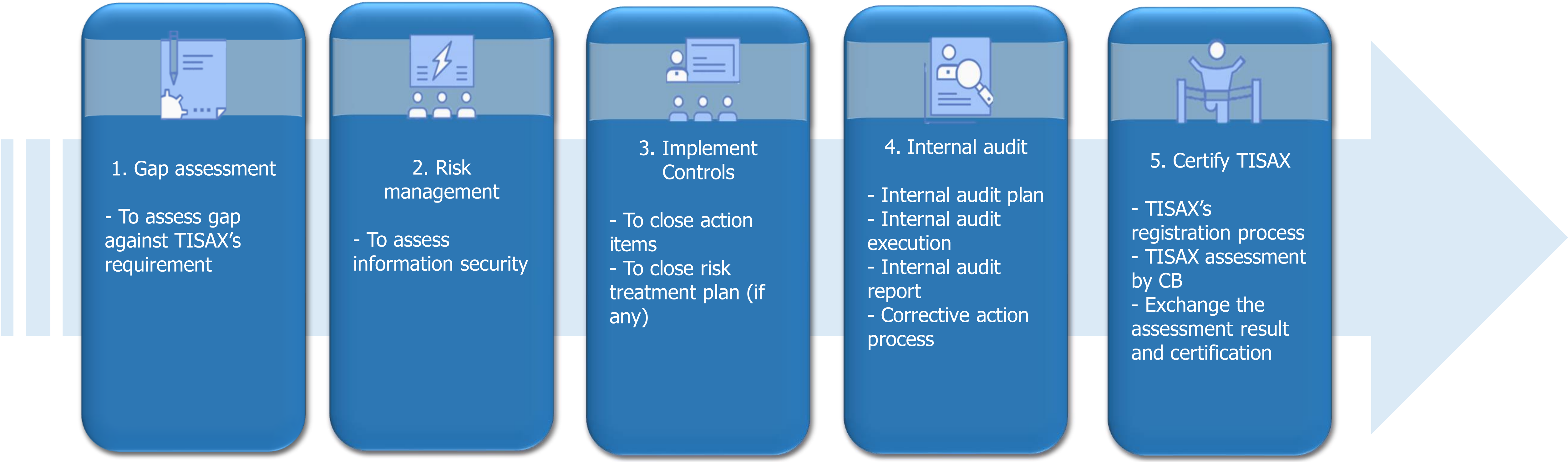
# TISAX requirements: Data Protection

9. Data Protection

## Implementation part

# TISAX implementation roadmap

# TISAX implementation roadmap : Option 1_TISAX [8 months]



1. Gap assessment

- To assess gap against TISAX's requirement

2. Risk management

- To assess information security

3. Implement Controls

- To close action items
- To close risk treatment plan (if any)

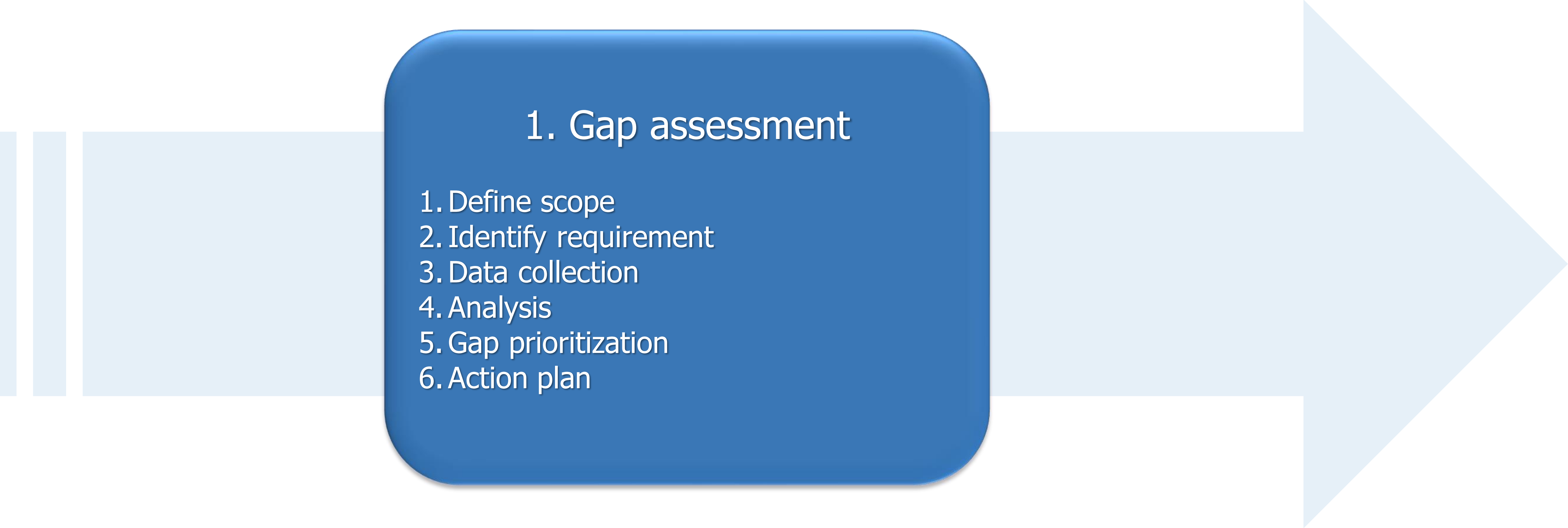
4. Internal audit

- Internal audit plan
- Internal audit execution
- Internal audit report
- Corrective action process

5. Certify TISAX

- TISAX's registration process
- TISAX assessment by CB
- Exchange the assessment result and certification

# TISAX implementation roadmap : Option 1_TISAX



## 1. Gap assessment

1. Define scope
2. Identify requirement
3. Data collection
4. Analysis
5. Gap prioritization
6. Action plan

# TISAX implementation roadmap : Option 1_TISAX

## 2. Risk management

1. Establish Governance and Leadership
2. Risk identification
3. Risk assessment
4. Risk mitigation
5. Risk monitoring
6. Reporting and Communication
7. Budget and Resource Allocation
8. Metrics and Key performance indicators (KPIs)

# TISAX implementation roadmap : Option 1_TISAX

## 3. Implement Controls

1. Develop policies and procedures
2. Implement people controls
3. Implement technical controls
4. Implement access controls
5. Implement physical controls
6. Implement data protection controls
7. Third party management
8. Monitor, detect and response security incidents
9. Business continuity management
10. Regularly assess and audit
11. Communication, Evaluation and Management support

# TISAX implementation roadmap : Option 1_TISAX

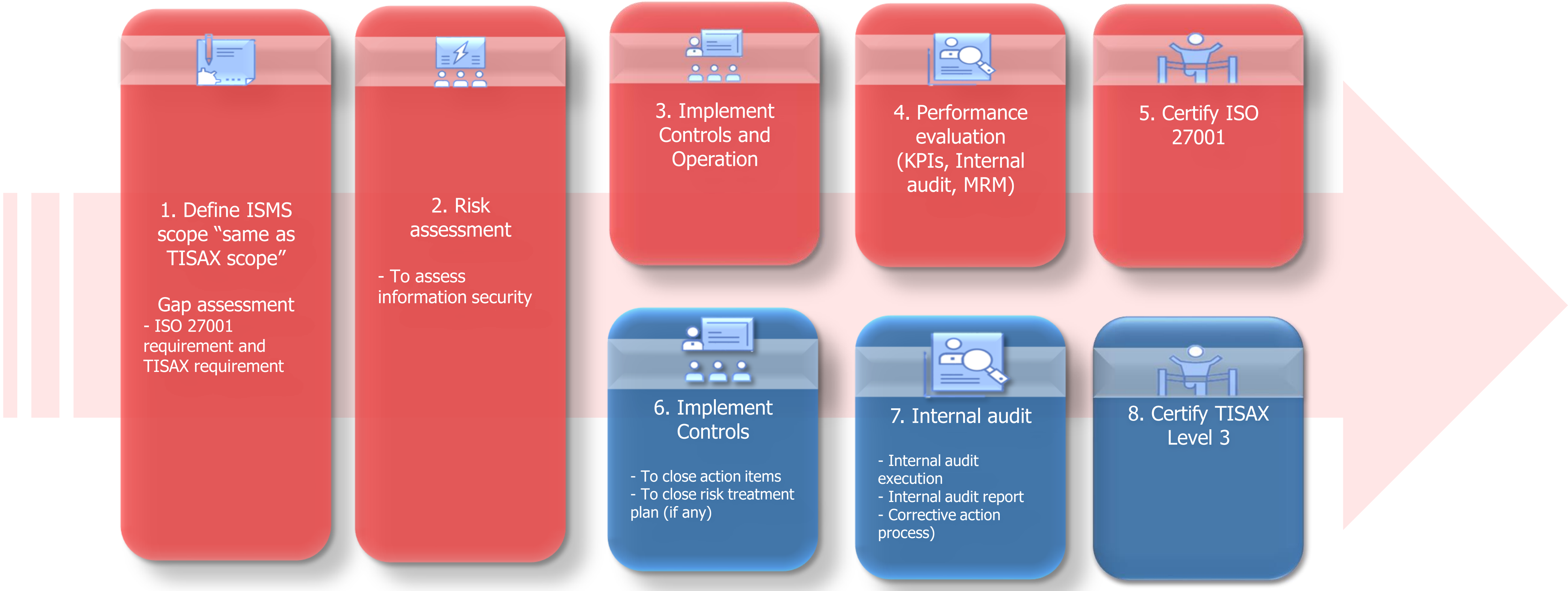
## 4. Internal audit

1. Planning
2. Audit criteria
3. Audit program (checklist, questionnaire)
4. Data collection
5. Audit execution
6. Analyze the data and evidence
7. Audit report
8. Present audit summary to management
9. Corrective action process

# TISAX implementation roadmap : Option 1_TISAX

Certify TISAX level 3

# TISAX implementation roadmap : Option 2_ISMS + TISAX [12 months]



1. Define ISMS scope "same as TISAX scope"

Gap assessment
- ISO 27001 requirement and TISAX requirement

2. Risk assessment

- To assess information security

3. Implement Controls and Operation

4. Performance evaluation (KPIs, Internal audit, MRM)

5. Certify ISO 27001

6. Implement Controls

- To close action items
- To close risk treatment plan (if any)

7. Internal audit

- Internal audit execution
- Internal audit report
- Corrective action process)

8. Certify TISAX Level 3

# TISAX implementation roadmap : Option 2_ISMS + TISAX

1. Define ISMS scope “same as TISAX scope”

Gap assessment

1. Identify requirement
2. Data collection
3. Analysis
4. Gap prioritization
5. Action plan

# TISAX implementation roadmap : Option 2_ISMS + TISAX

2. Risk management

1. Establish Governance and Leadership
2. Risk identification
3. Risk assessment
4. Risk mitigation
5. Risk monitoring
6. Reporting and Communication
7. Budget and Resource Allocation
8. Metrics and Key performance indicators (KPIs)

# TISAX implementation roadmap : Option 2_ISMS + TISAX

## 3. Implement Controls

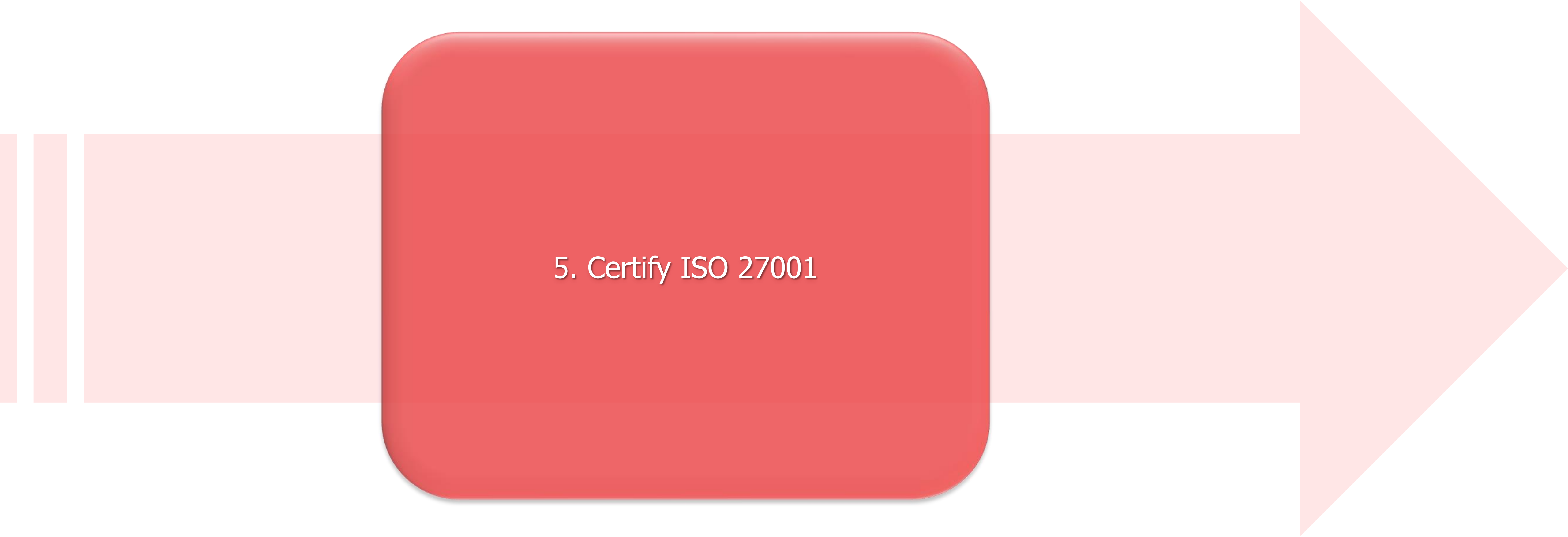
1. Develop policies and procedures
2. Implement people controls
3. Implement technical controls
4. Implement access controls
5. Implement physical controls
6. Implement data protection controls
7. Third party management
8. Monitor, detect and response security incidents
9. Business continuity management
10. Regularly assess and audit
11. Communication, Evaluation and Management support

# TISAX implementation roadmap : Option 2_ISMS + TISAX

4. Performance evaluation

1. Define Objectives and Metrics
2. Measure Performance
3. Monitor and Analyze Data
4. Corrective and Preventive Actions
5. Continual Improvement

# TISAX implementation roadmap : Option 2_ISMS + TISAX



5. Certify ISO 27001

# TISAX implementation roadmap : Option 1_TISAX

6. Implement Controls

1. Develop policies and procedures
2. Implement people controls
3. Implement technical controls
4. Implement access controls
5. Implement physical controls
6. Implement data protection controls
7. Third party management
8. Monitor, detect and response security incidents
9. Business continuity management
10. Regularly assess and audit
11. Communication, Evaluation and Management support

# TISAX implementation roadmap : Option 1_TISAX

7. Internal audit

1. Planning
2. Audit criteria
3. Audit program (checklist, questionnaire)
4. Data collection
5. Audit execution
6. Analyze the data and evidence
7. Audit report
8. Present audit summary to management
9. Corrective action process

# TISAX implementation roadmap : Option 1_TISAX

8. Certify TISAX level 3

# Implementation part

## Key takeaways

## ISMS ISO 27001

- ISO 27001 is a globally recognized standard that provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within an organization
- ISO 27001 is applicable to a wide range of organizations across different industries, not limited to automotive
- The certification program by CB auditor is not specific to any industry
- ISO 27001 is a broad information security management standard applicable to various industries

## TISAX

- TISAX is a specific assessment and exchange mechanism primarily used in the automotive industry
- TISAX is industry-specific and mainly used by automotive manufacturers and their suppliers. It was developed to standardize information security assessments within the automotive supply chain.
- TISAX assessments are typically conducted by authorized audit providers who are trained and approved by the automotive industry
- TISAX places a strong emphasis on data protection and includes requirements specific to the automotive industry's data handling and protection requirements.

*** 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.*

# Benefits of TISAX

- Standardizes automotive-specific requirements for information security
- Cross-company recognition of the assessment results amongst all TISAX® participants
- Effective risk management strategies and Provides efficiencies for manufacturers and suppliers
- Higher credibility for certified organization between suppliers and customers

- Mutual recognition in the TISAX® network saves time and cost
- Better clarity due to harmonized VDA-ISA test catalog
- Effective risk management strategies and Provides efficiencies for manufacturers and suppliers
- Business development opportunities thanks to industry-wide recognition

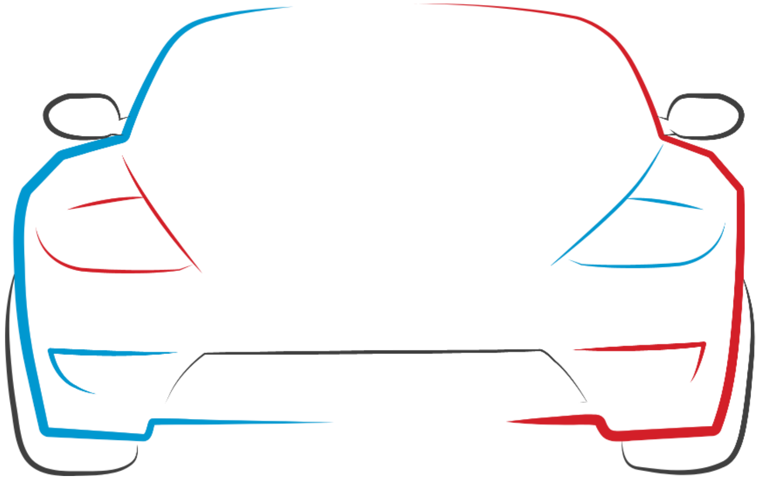
# Agenda

## Implementation part

1. What's TISAX? and Why TISAX?
2. The TISAX process and Scope of TISAX
3. TISAX requirements
4. TISAX implementation roadmap
5. Key takeaways

## Audit part

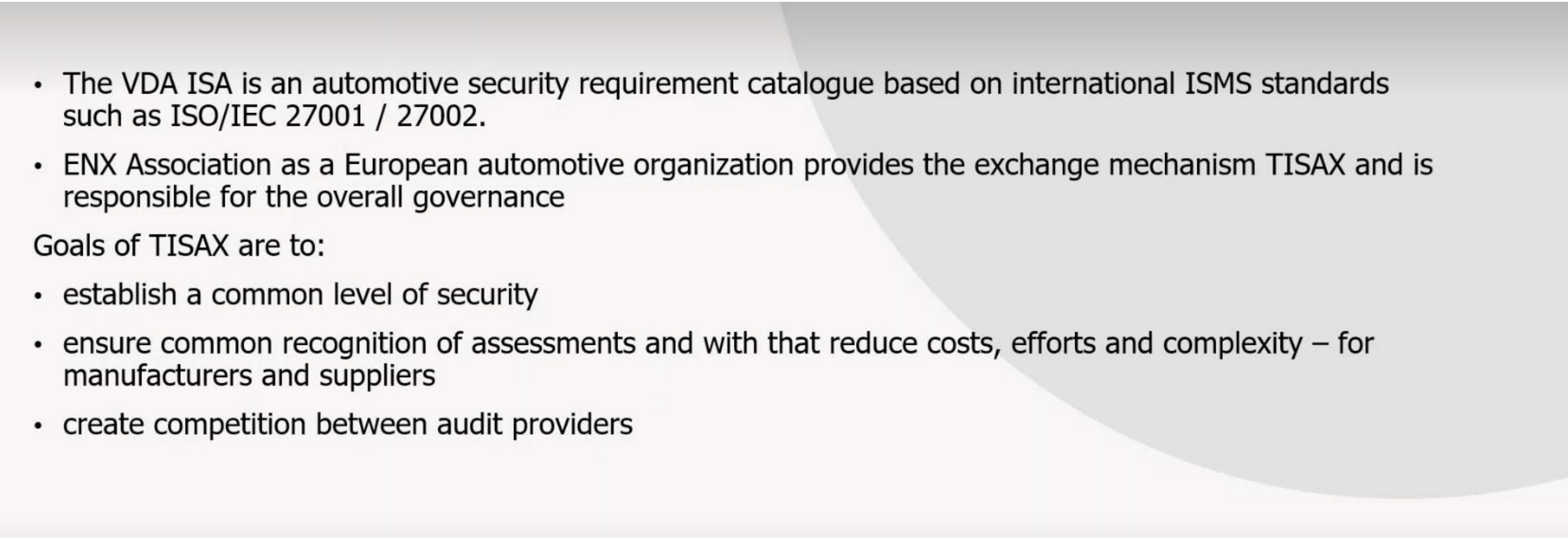
1. Why is TISAX certified?
2. TISAX assessment level
3. TISAX assessment process
4. TISAX certification maintenance program
5. Key takeaways



# Audit part

## Why is TISAX certified?

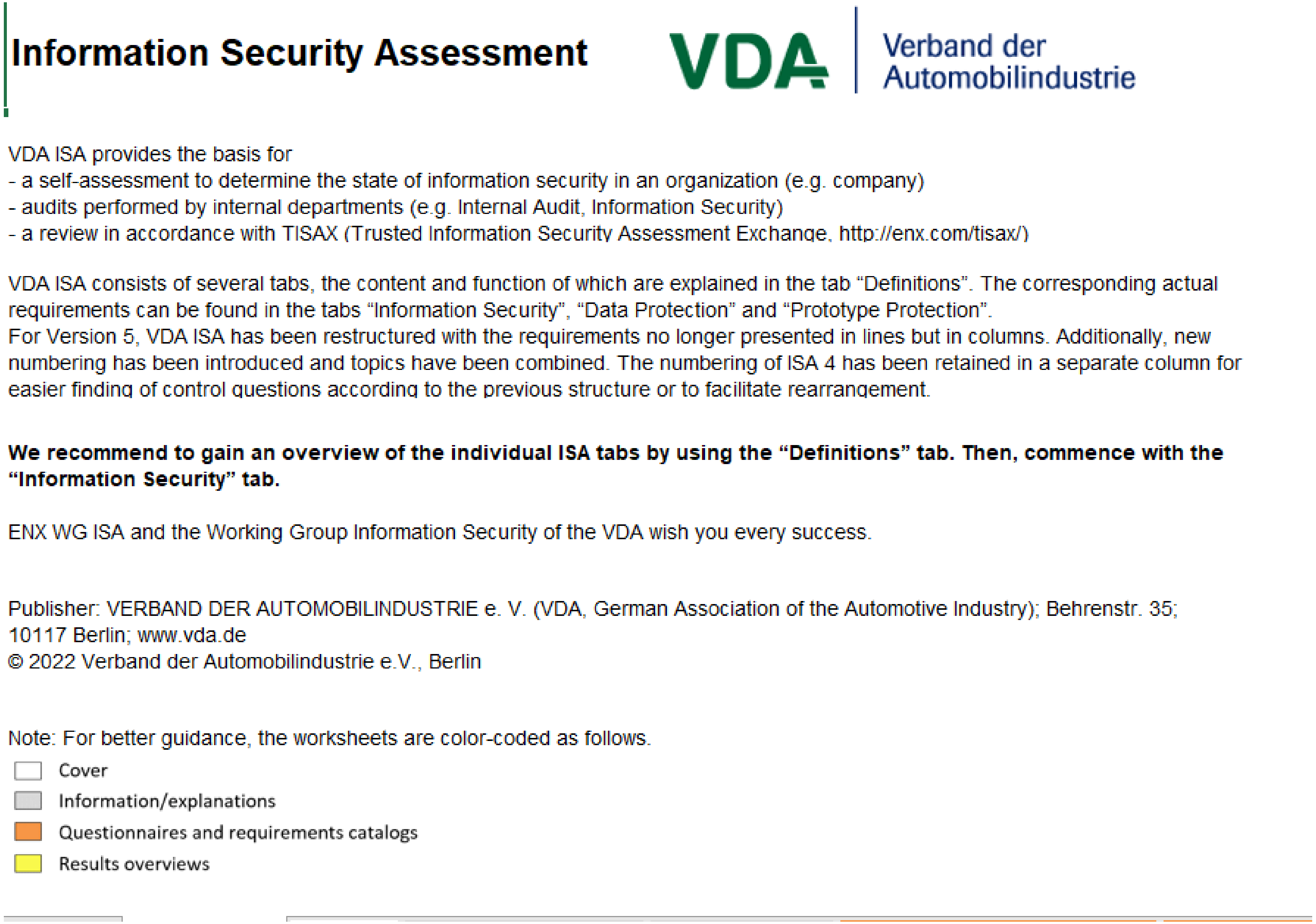
# TISAX Purpose and Goals



- The VDA ISA is an automotive security requirement catalogue based on international ISMS standards such as ISO/IEC 27001 / 27002.
- ENX Association as a European automotive organization provides the exchange mechanism TISAX and is responsible for the overall governance

Goals of TISAX are to:

- establish a common level of security
- ensure common recognition of assessments and with that reduce costs, efforts and complexity – for manufacturers and suppliers
- create competition between audit providers



# Information Security Assessment

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.**

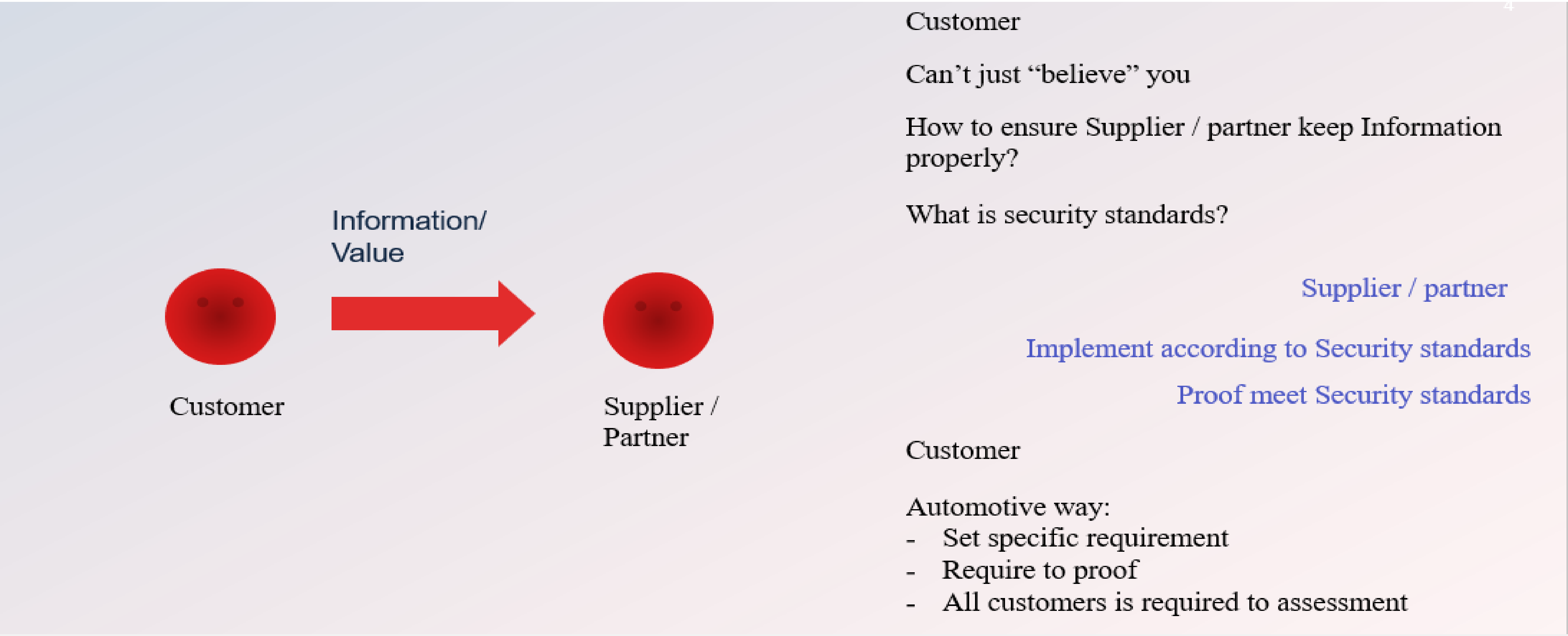
ENX WG ISA and the Working Group Information Security of the VDA wish you every success.

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

Note: For better guidance, the worksheets are color-coded as follows.

□ Cover
▨ Information/explanations
🟧 Questionnaires and requirements catalogs
🟨 Results overviews

# Trusted information security



Information/ Value

Customer

Supplier / Partner

Customer

Can’t just “believe” you

How to ensure Supplier / partner keep Information properly?

What is security standards?

Supplier / partner

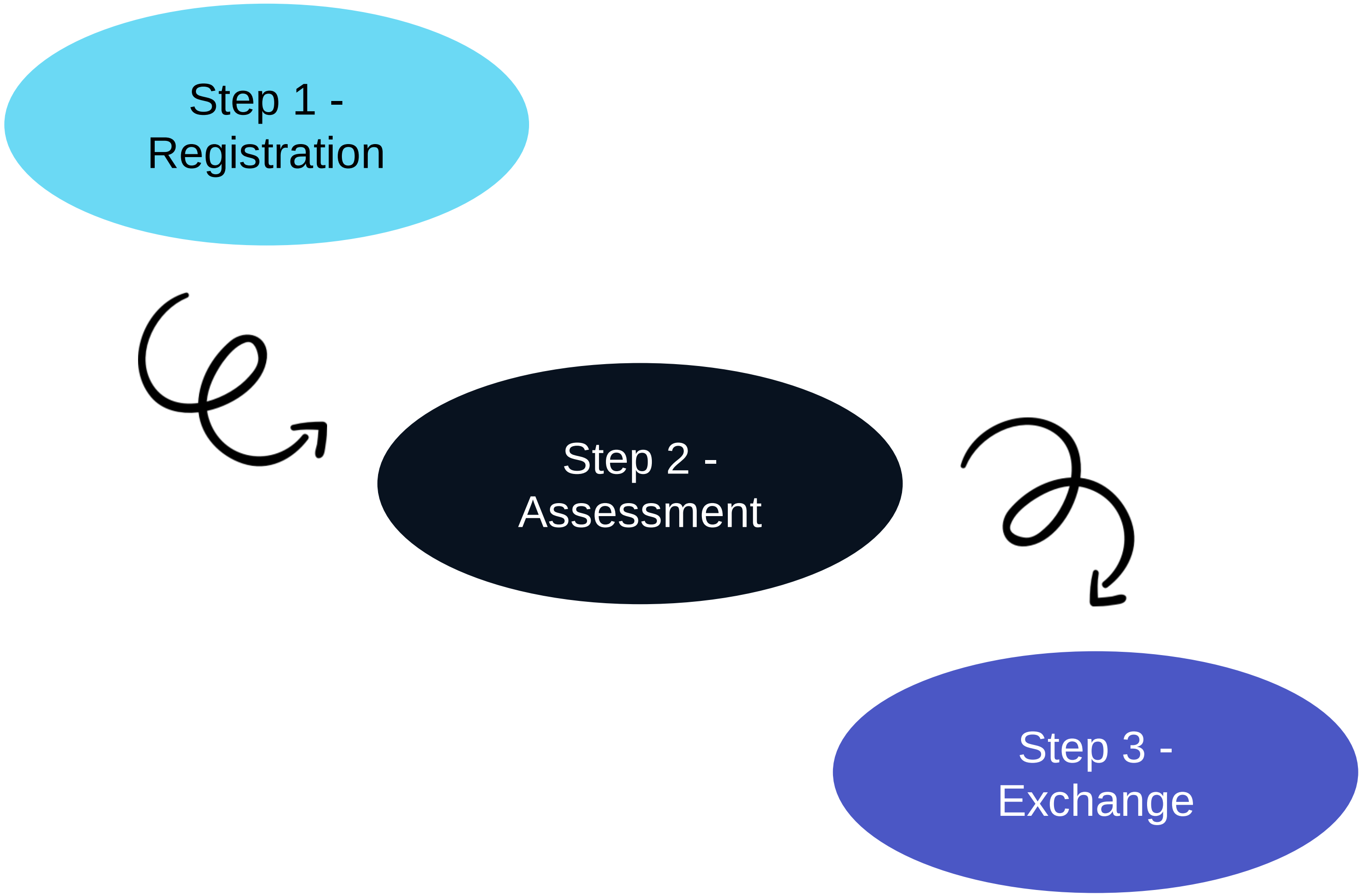
Implement according to Security standards

Proof meet Security standards

Customer

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

# The TISAX process

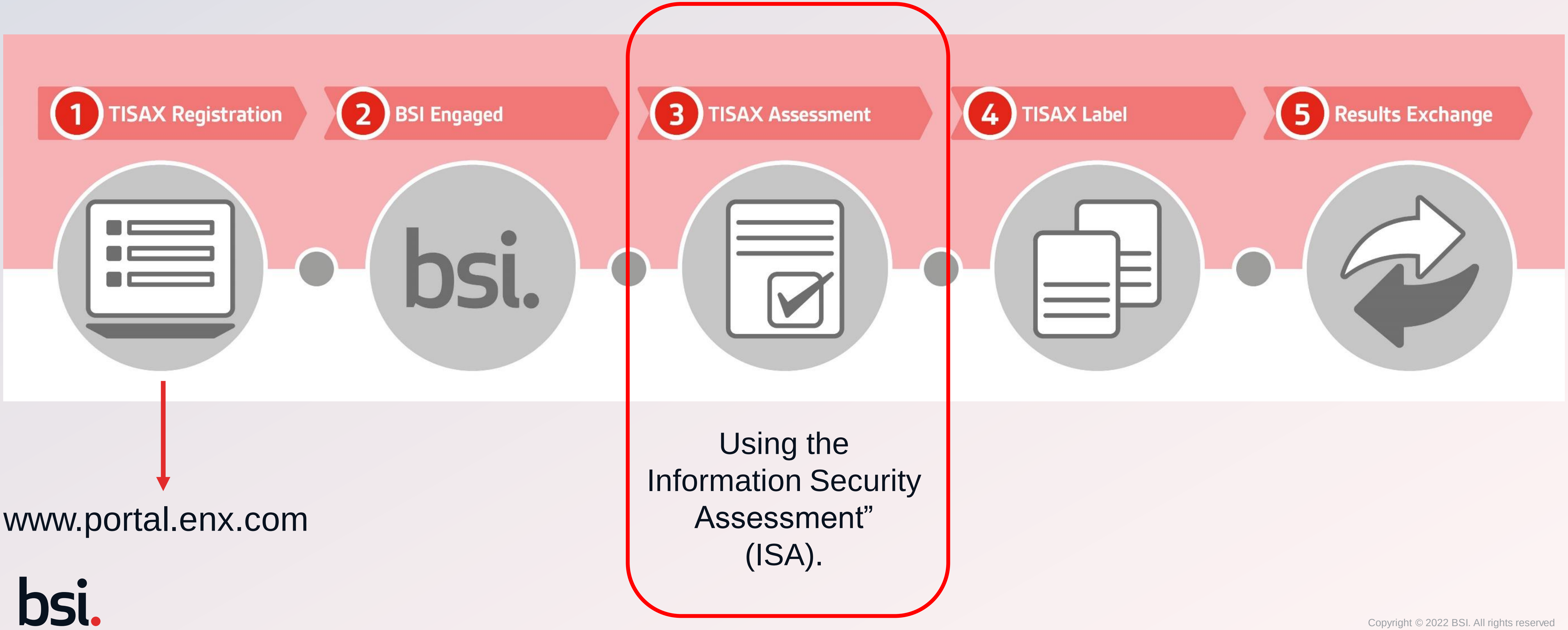


Step 1 - Registration

Step 2 - Assessment

Step 3 - Exchange

# The TISAX process – how to obtain the label

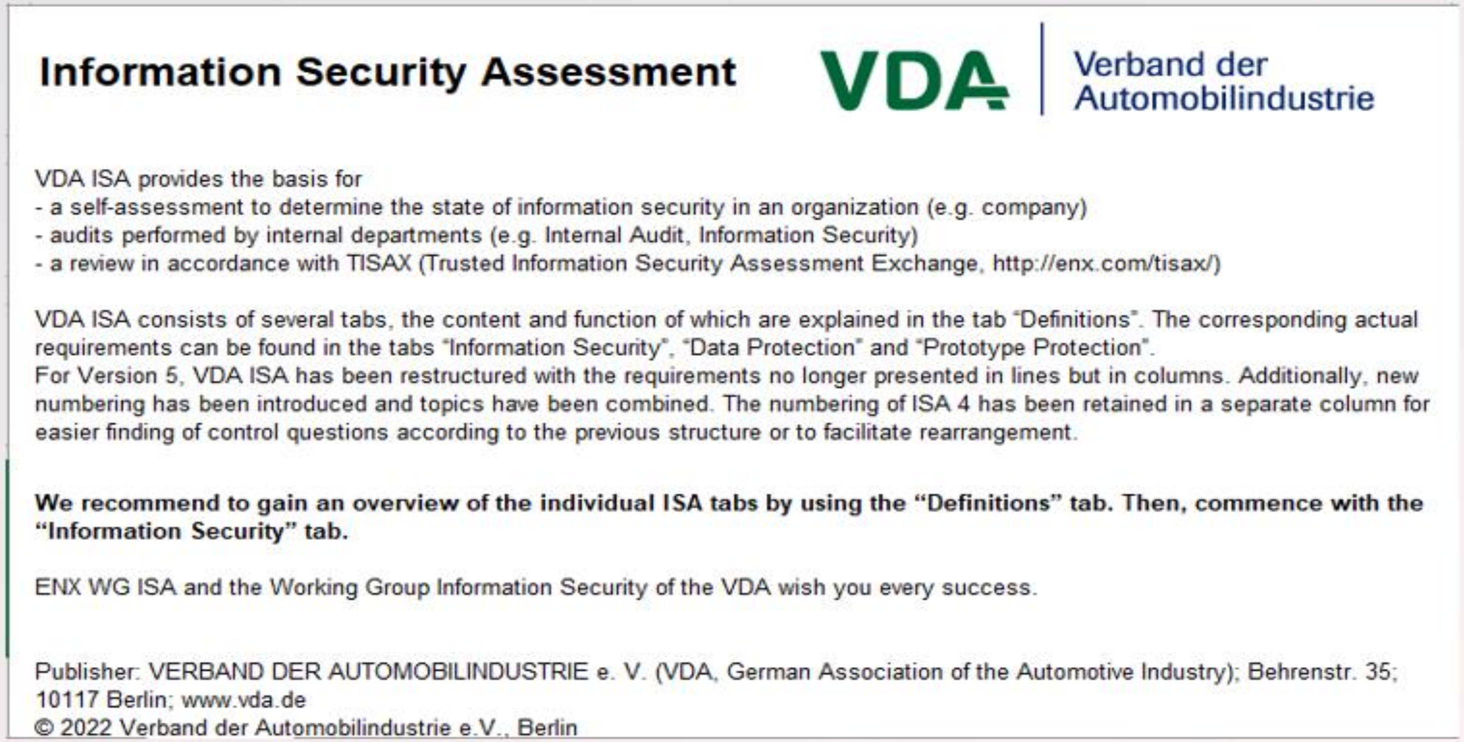


www.portal.enx.com

Using the Information Security Assessment” (ISA).

# About Audit

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



## Information Security Assessment

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.

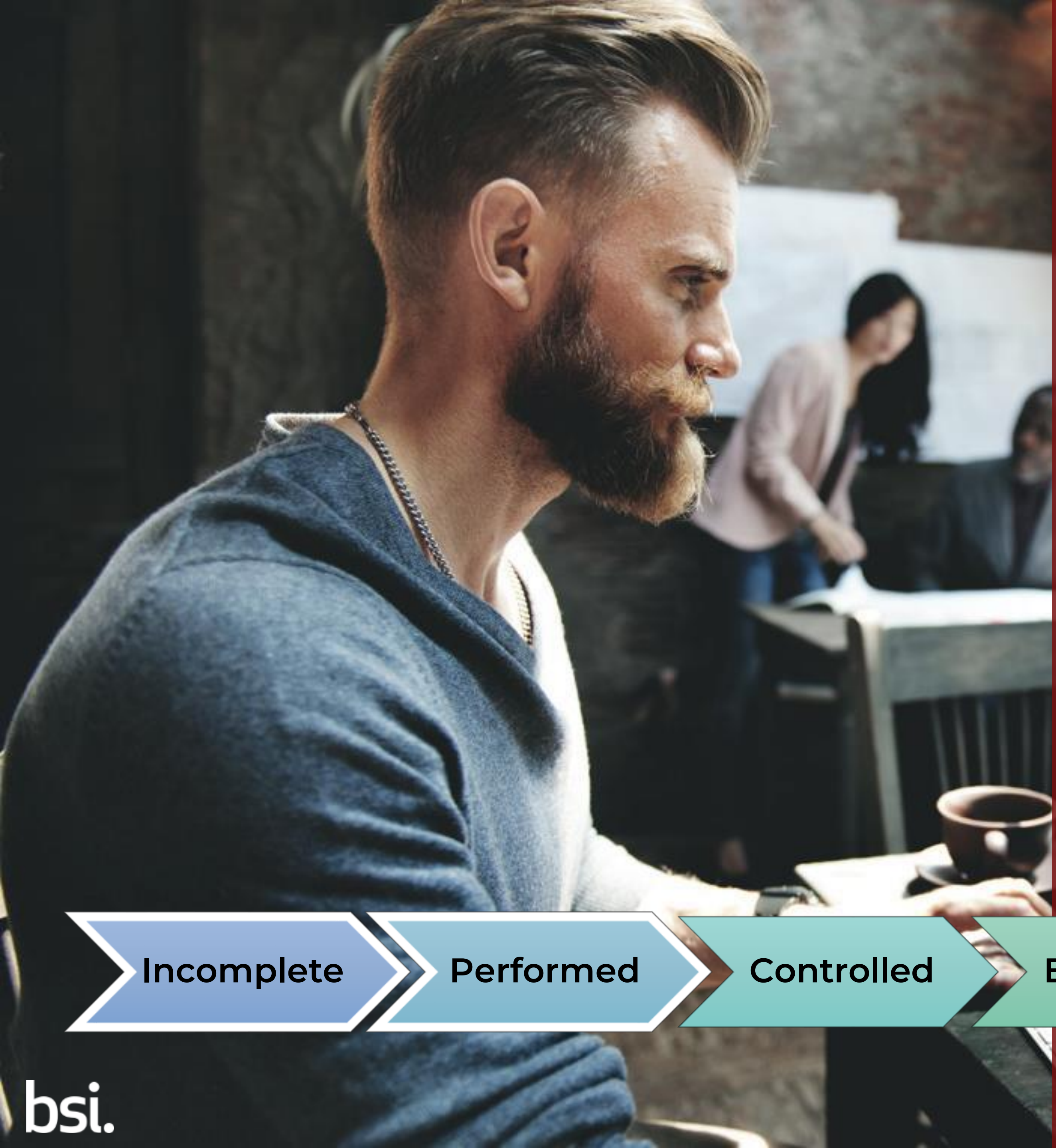
**We recommend to gain an overview of the individual ISA tabs by using the "Definitions" tab. Then, commence with the "Information Security" tab.**

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
© 2022 Verband der Automobilindustrie e.V., Berlin

# Audit part

## TISAX assessment level



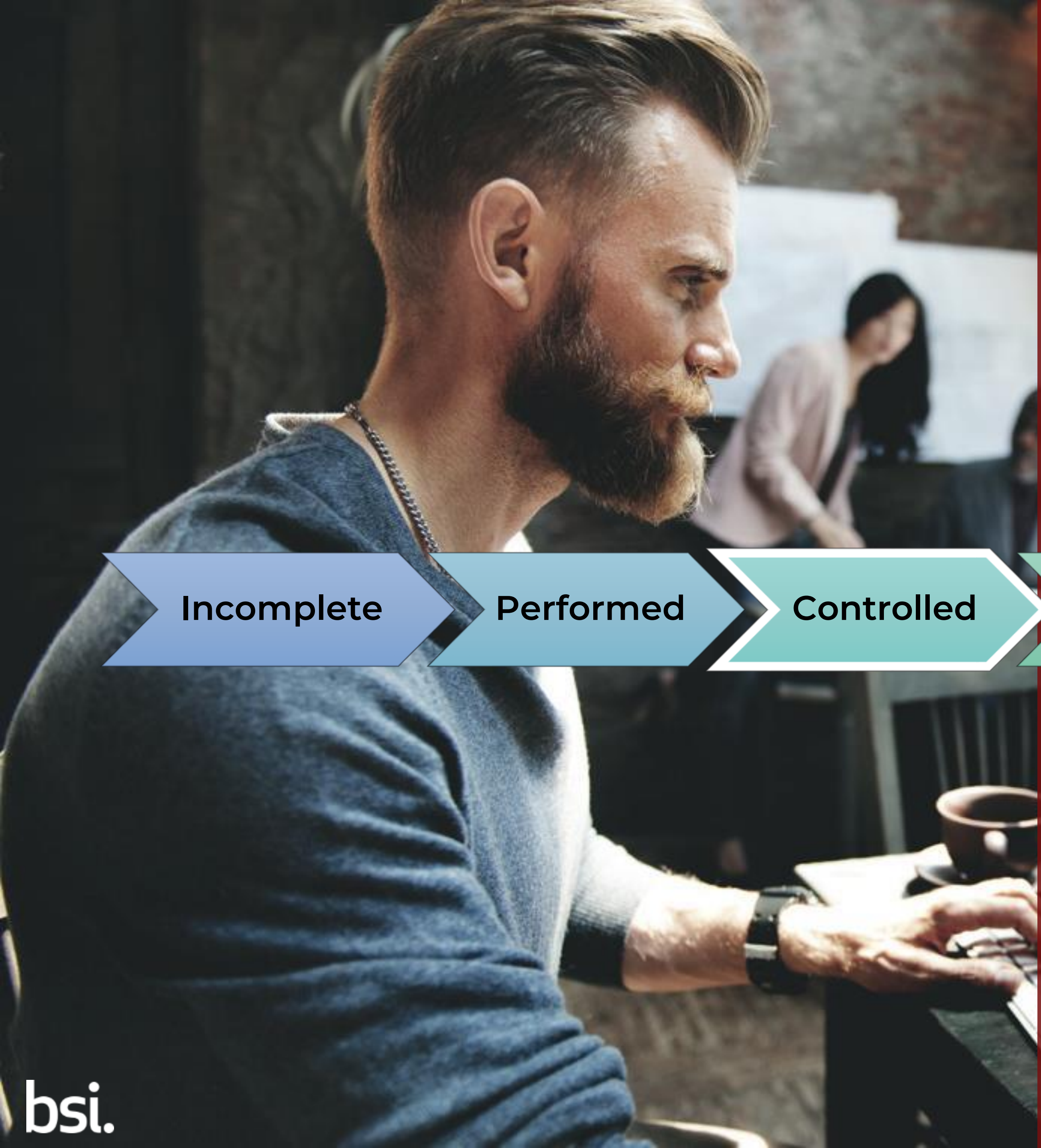
# Maturity levels

The maturity levels describe the quality of implementation and **must** be supported by evidence

Average per catalogue determines overall maturity level and the results tells you if you are ready for the audit

Incomplete → Performed → Controlled → Established → Predictablle → Optimizing

bsi.



# Maturity levels

Incomplete → Performed → Controlled → Established → Predictablle → Optimizing

# Maturity levels

Incomplete

Performed

Controlled

Established

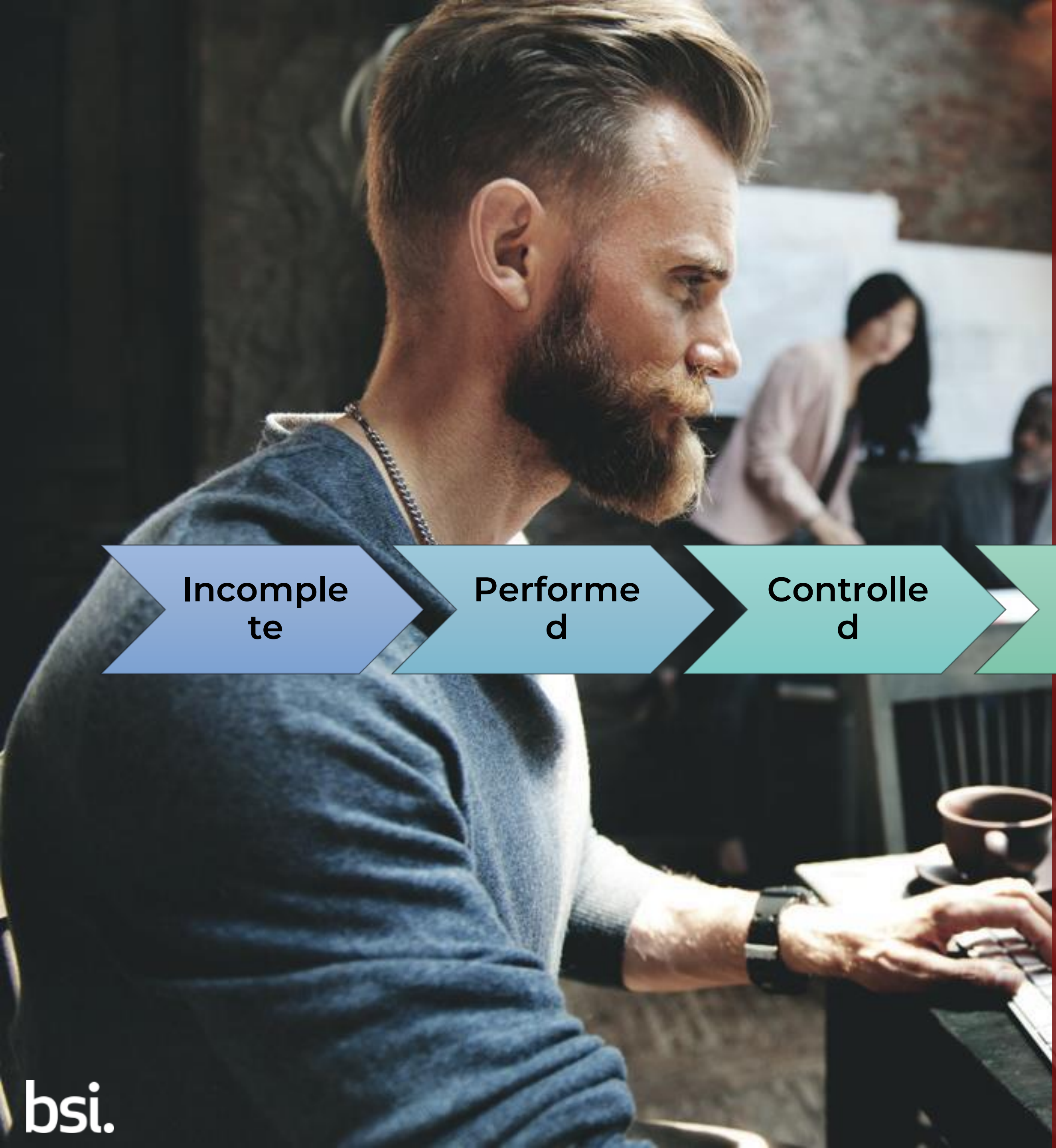
Predictablle

Optimizing

# Maturity levels

Incomplete → Performed → Controlled → Established → Predictablle → Optimizing

# Maturity levels



Incomplete

Performed

Controlled

Established

Predictablle

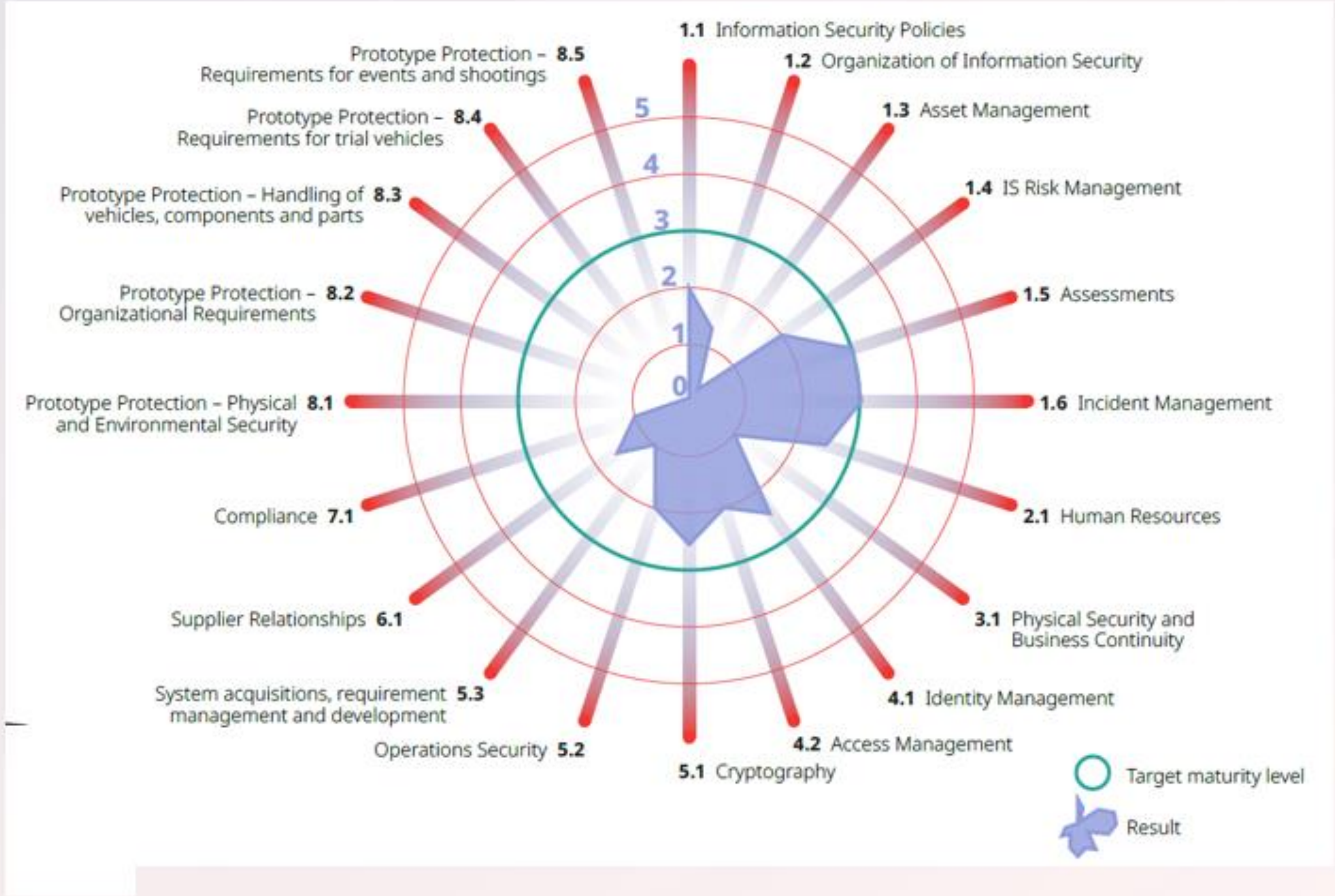
Optimizing

# Maturity

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.

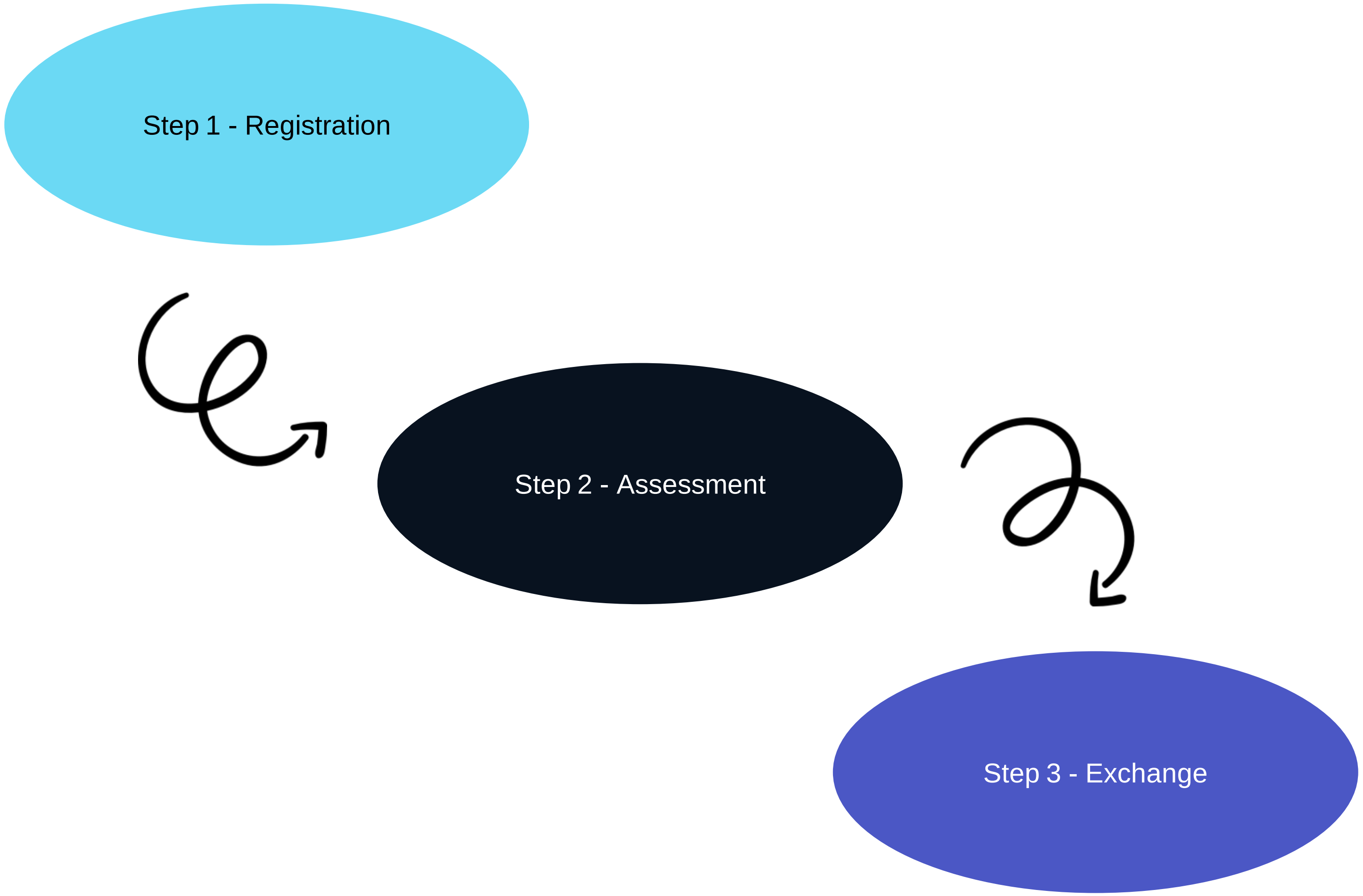
TISAX labels can then be exchanged with other registered participants in the ENX Portal.



# Audit part

## TISAX assessment process

# The TISAX process



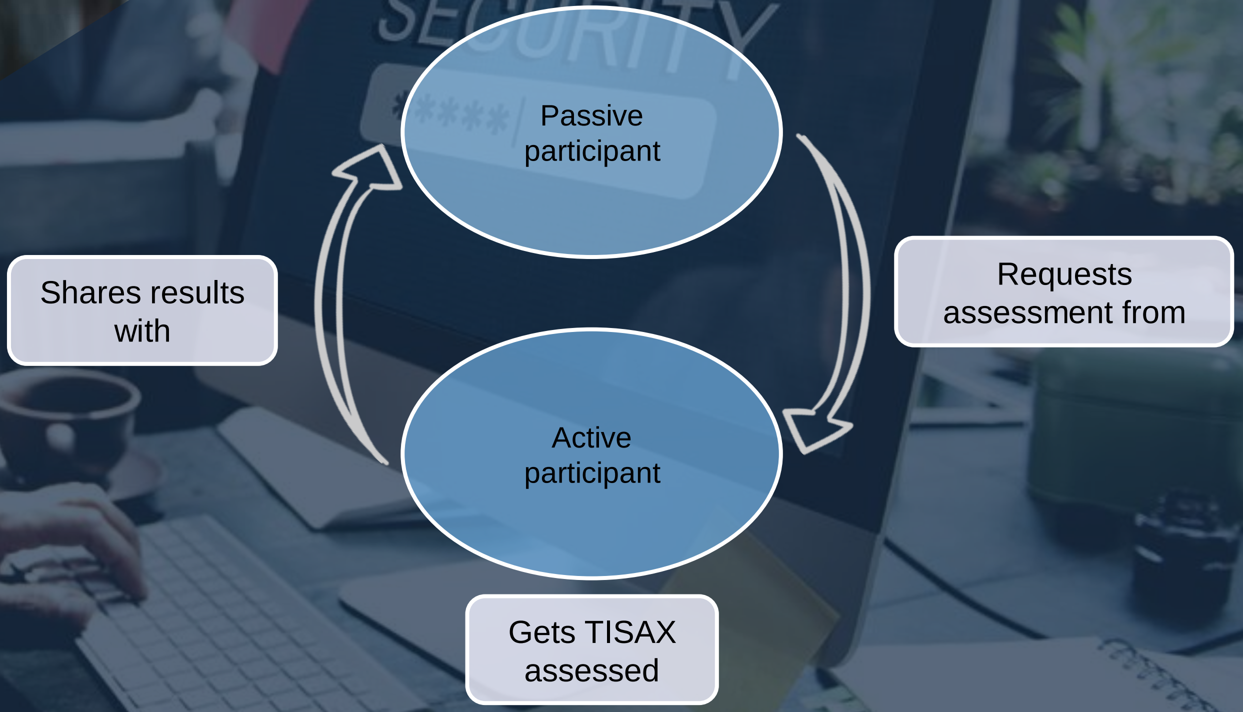
Step 1 - Registration

Step 2 - Assessment

Step 3 - Exchange

# Step 1
# Registration

Customers and suppliers both registered as a “participant”



Passive participant

Requests assessment from

Active participant

Gets TISAX assessed

Shares results with

An organization can be registered as both an active and passive participant.

# The TISAX assessment scope

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**:

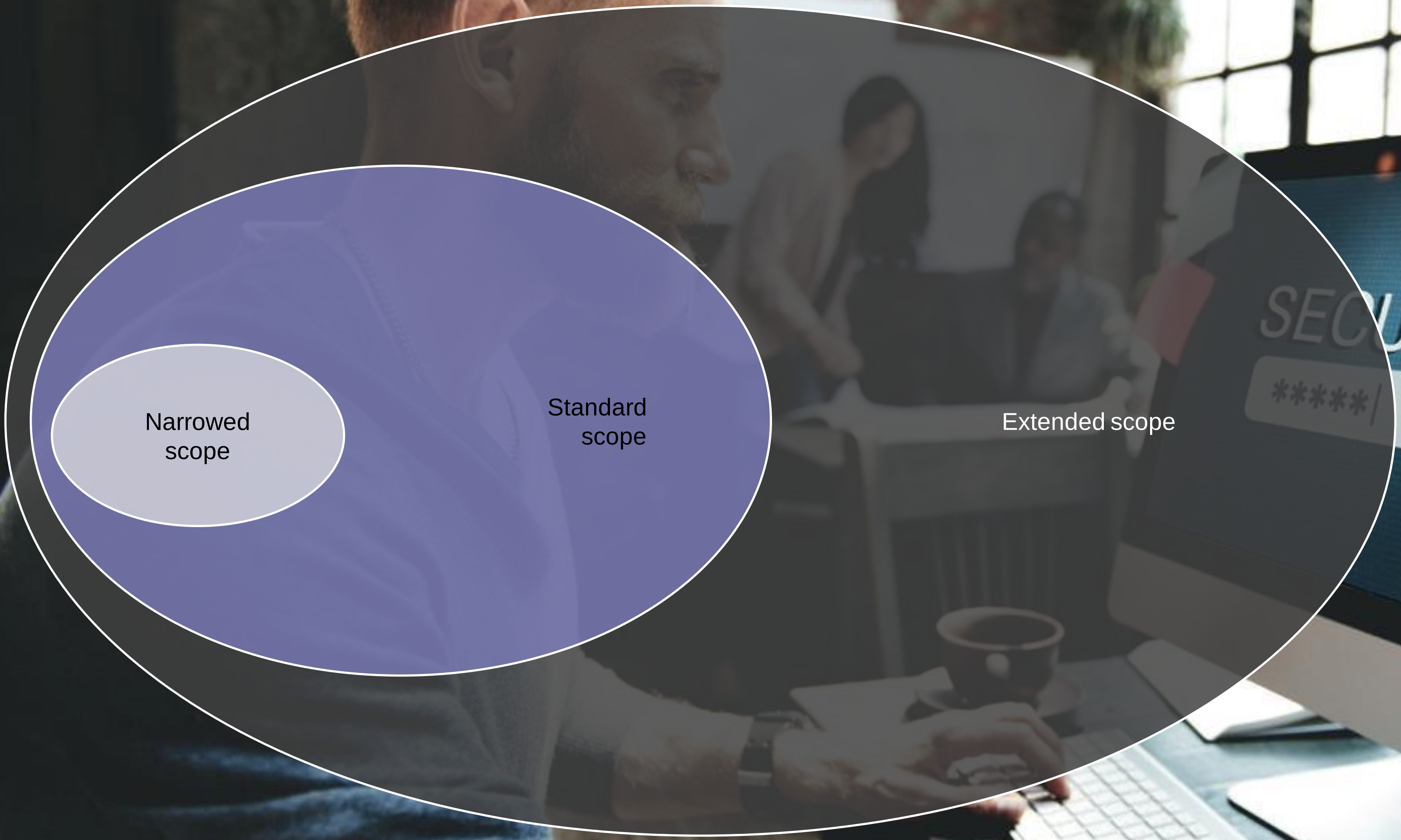
- Work equipment
- Employees
- IT systems including cloud services such as infrastructure/ platform/software as a service
- Physical sites
- Relevant contractors

**Examples for sites:**

- Office sites
- Development sites
- Production sites
- Data centres

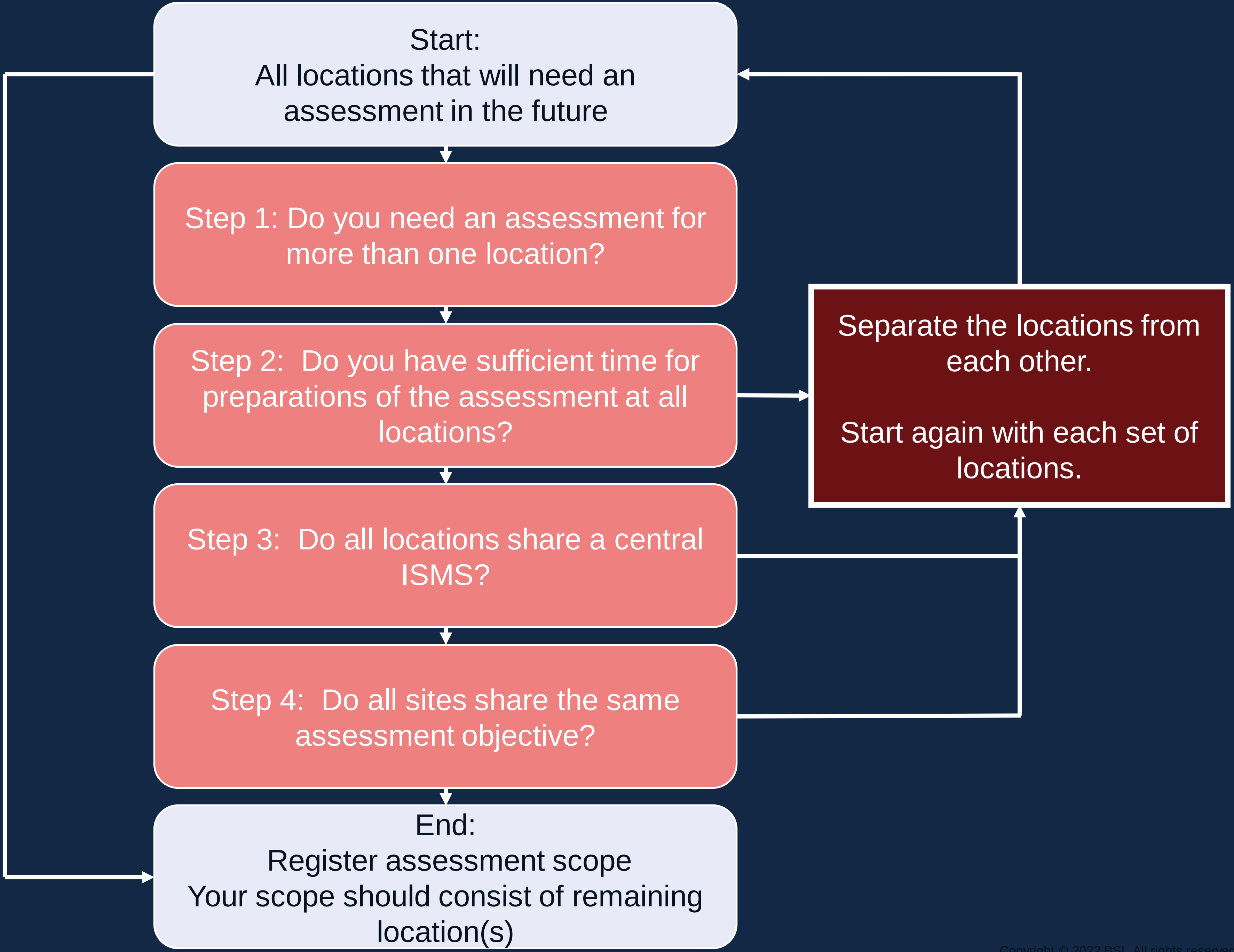
bsi.

# Custom scoping



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

# Scoping



Start:
All locations that will need an assessment in the future

Step 1: Do you need an assessment for more than one location?

Step 2: Do you have sufficient time for preparations of the assessment at all locations?

Step 3: Do all locations share a central ISMS?

Step 4: Do all sites share the same assessment objective?

End:
Register assessment scope
Your scope should consist of remaining location(s)

Separate the locations from each other.

Start again with each set of locations.

# Assessment objectives

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

- Information security
- Prototype protection
- Data protection

1 **Info high** – Information with high protection needs

2 **Info very high** – Information with very high protection needs

3 **Proto parts** – Protection of prototype parts and components

4 **Proto vehicles** – Protection of prototype vehicles

5 **Test vehicles** – Handling of test vehicles

6 **Events and shootings** – Protection of prototypes during events and film or photo shootings

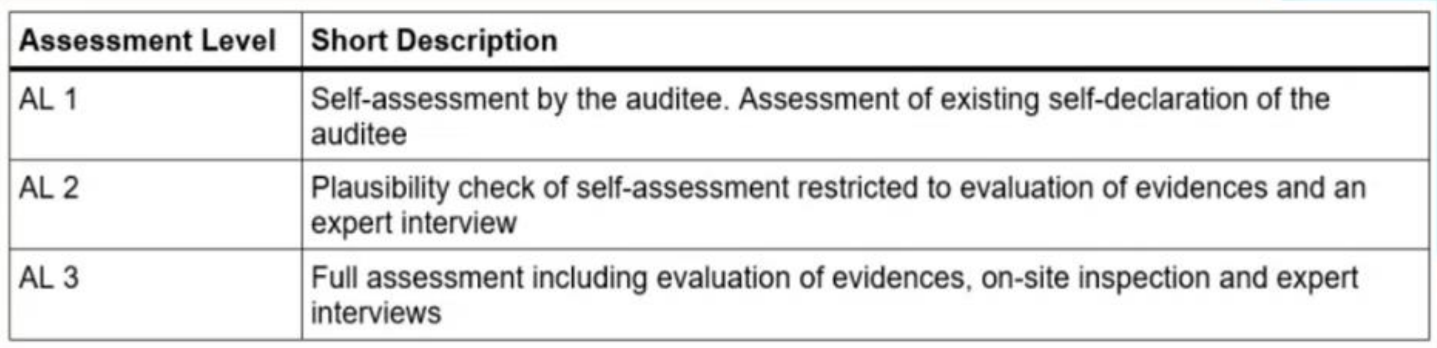
7 **Data** – Data protection. According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)

8 **Special data** – 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)

# TISAX Assessments Levels

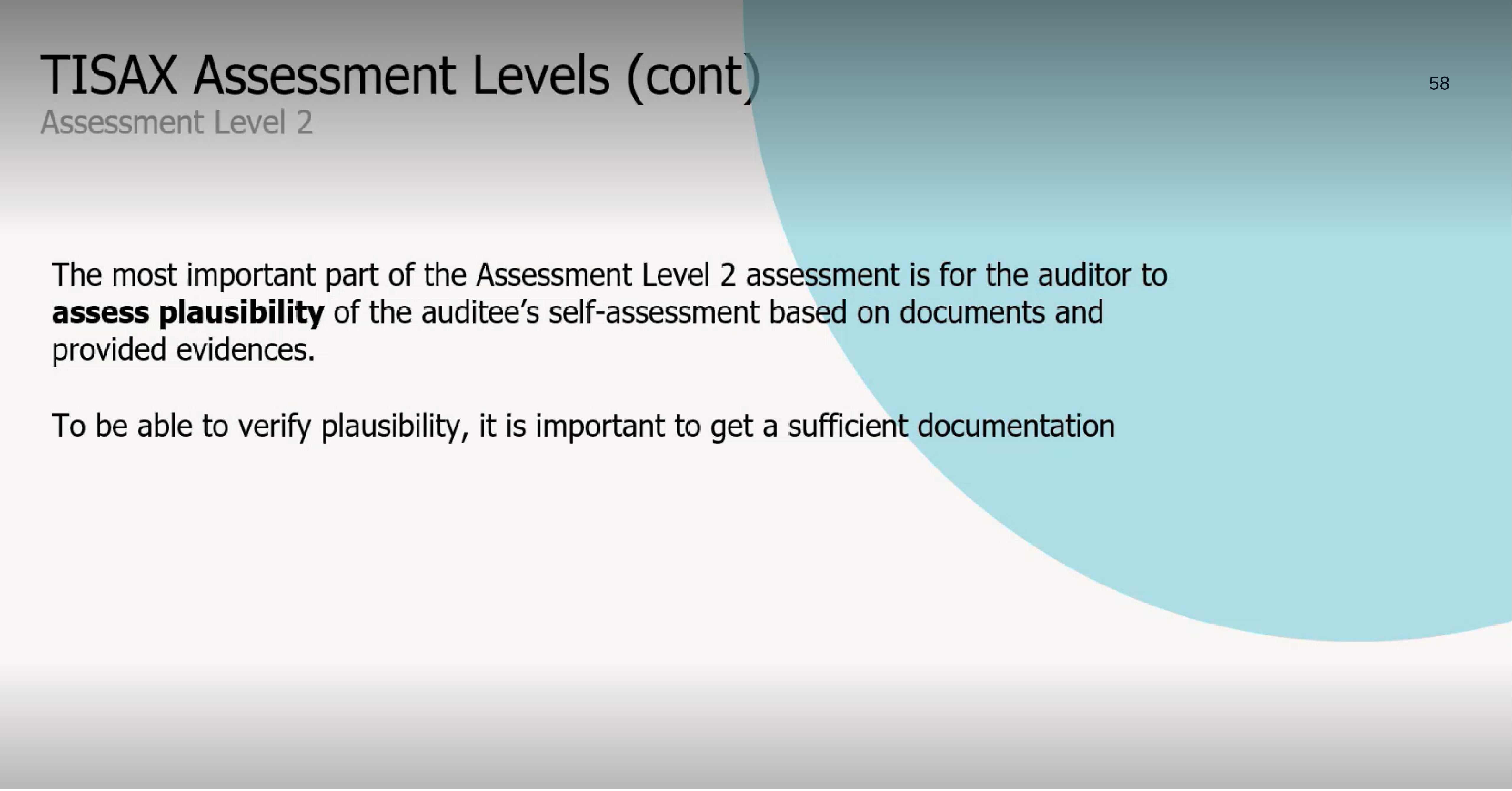
## Overview

TISAX consists of three different Assessment Levels (AL)



| Assessment Level | Short Description |
|---|---|
| AL 1 | Self-assessment by the auditee. Assessment of existing self-declaration of the auditee |
| AL 2 | Plausibility check of self-assessment restricted to evaluation of evidences and an expert interview |
| AL 3 | Full assessment including evaluation of evidences, on-site inspection and expert interviews |

As AL1 is only used for a special case of a simplified group assessment, it will not be described on the next pages

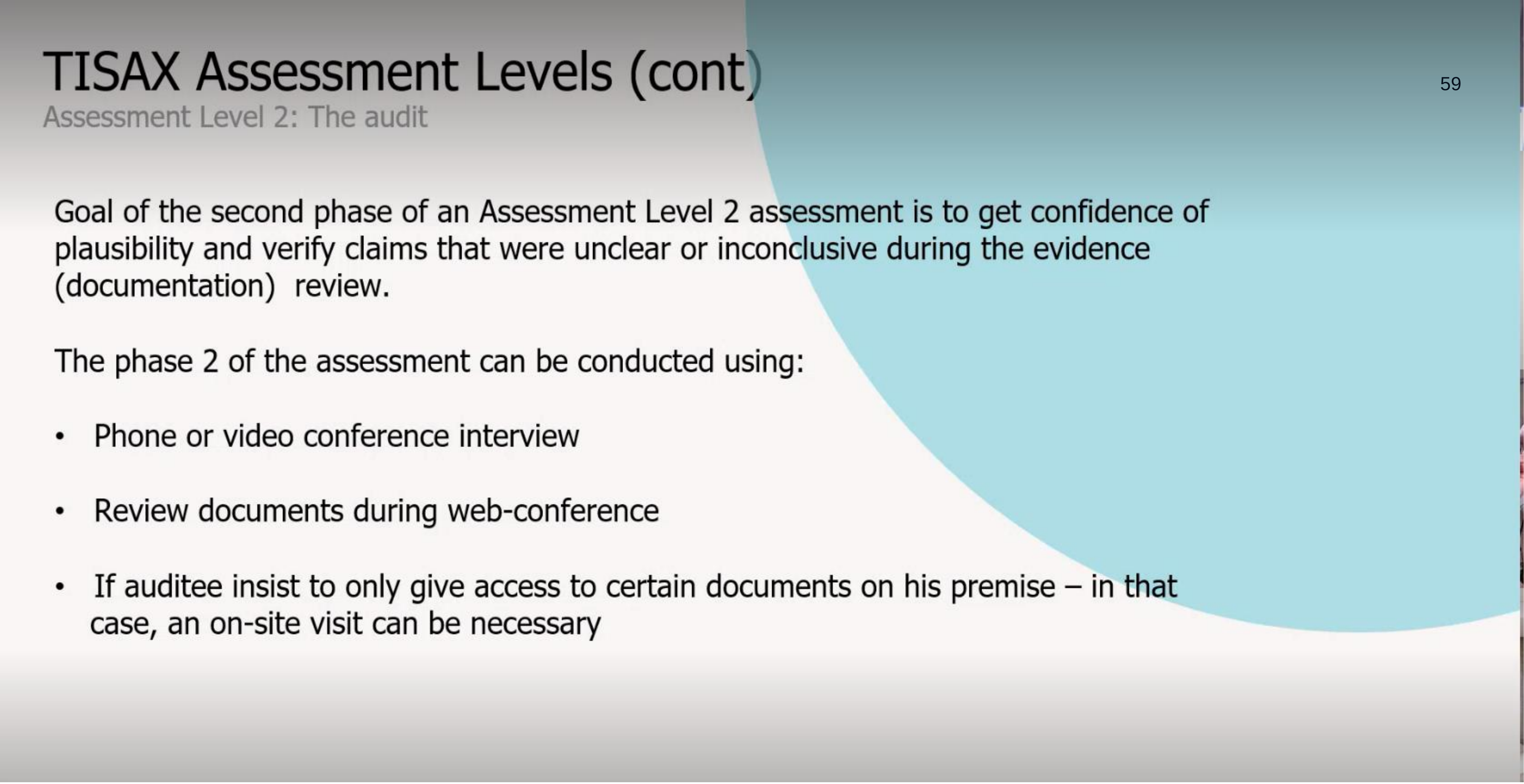


# TISAX Assessment Levels (cont)

## Assessment Level 2

The most important part of the Assessment Level 2 assessment is for the auditor to **assess plausibility** of the auditee’s self-assessment based on documents and provided evidences.

To be able to verify plausibility, it is important to get a sufficient documentation



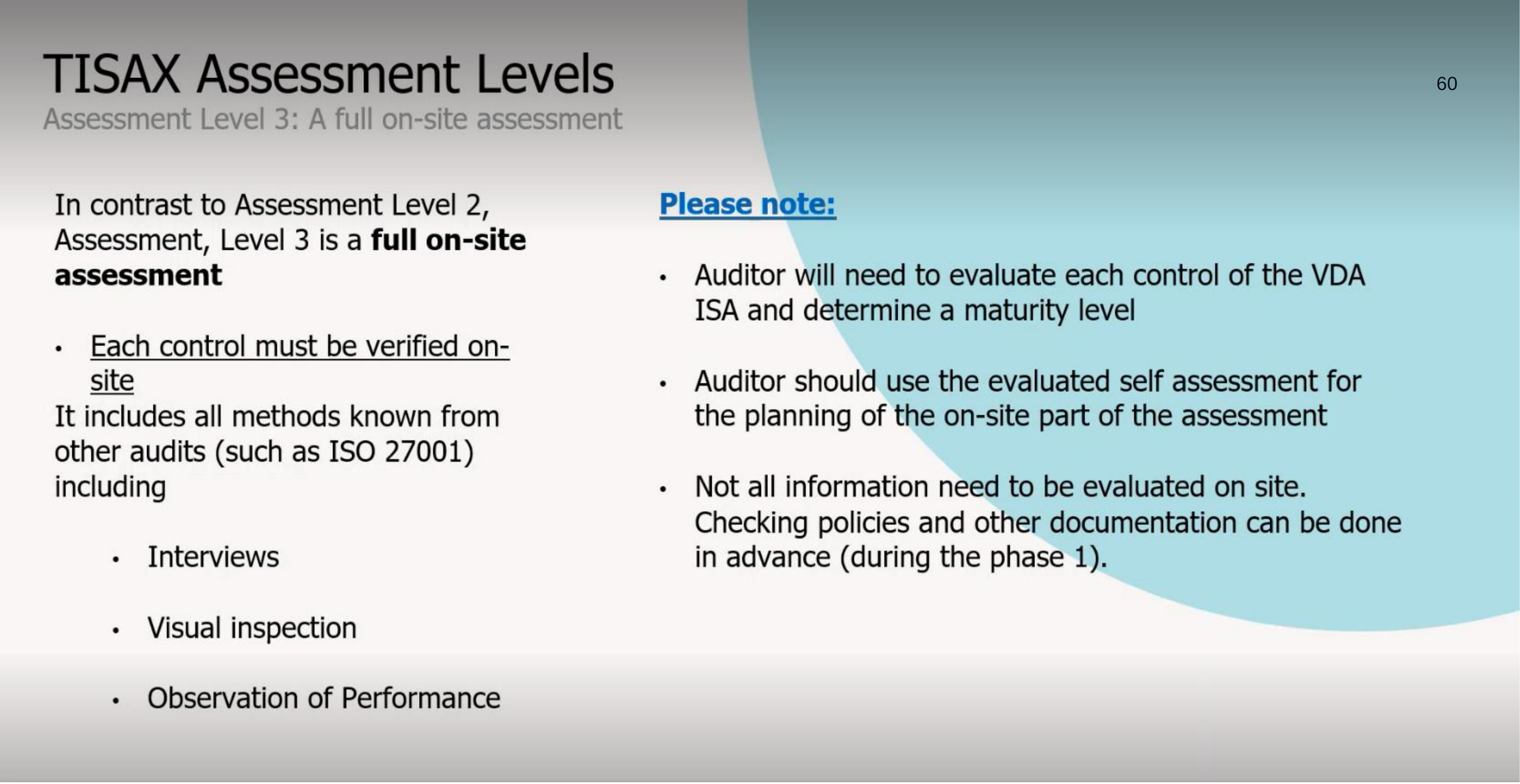
# TISAX Assessment Levels (cont)

## Assessment Level 2: The audit

Goal of the second phase of an Assessment Level 2 assessment is to get confidence of plausibility and verify claims that were unclear or inconclusive during the evidence (documentation) review.

The phase 2 of the assessment can be conducted using:

- Phone or video conference interview
- Review documents during web-conference
- If auditee insist to only give access to certain documents on his premise – in that case, an on-site visit can be necessary



# TISAX Assessment Levels

## Assessment Level 3: A full on-site assessment

In contrast to Assessment Level 2, Assessment, Level 3 is a **full on-site assessment**

- Each control must be verified on-site

It includes all methods known from other audits (such as ISO 27001) including

  - Interviews
  - Visual inspection
  - Observation of Performance

**Please note:**

- Auditor will need to evaluate each control of the VDA ISA and determine a maturity level
- Auditor should use the evaluated self assessment for the planning of the on-site part of the assessment
- Not all information need to be evaluated on site. Checking policies and other documentation can be done in advance (during the phase 1).

# Assessment levels

## Level 1

- For internal purposes in the true sense of a self-assessment
- An auditor checks for the existence of a completed self-assessment. They do not assess the content of the self-assessment. They do not require further evidence
- Results 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

## Level 2

- The audit provider does a plausibility check on your self-assessment (for allocations within the assessment scope). He supports this by checking evidence and conducting interviews with you and further colleagues
- The audit provider does the interviews generally via audio conference. At your request, they can conduct the interviews in person
- Generally does not include an on-site inspection, however, assessments always include an on-site inspection if you have selected one of the “prototype” assessment objectives
- If you have evidence you don’t want to send to the audit provider, you can request an on-site inspection

## Level 3

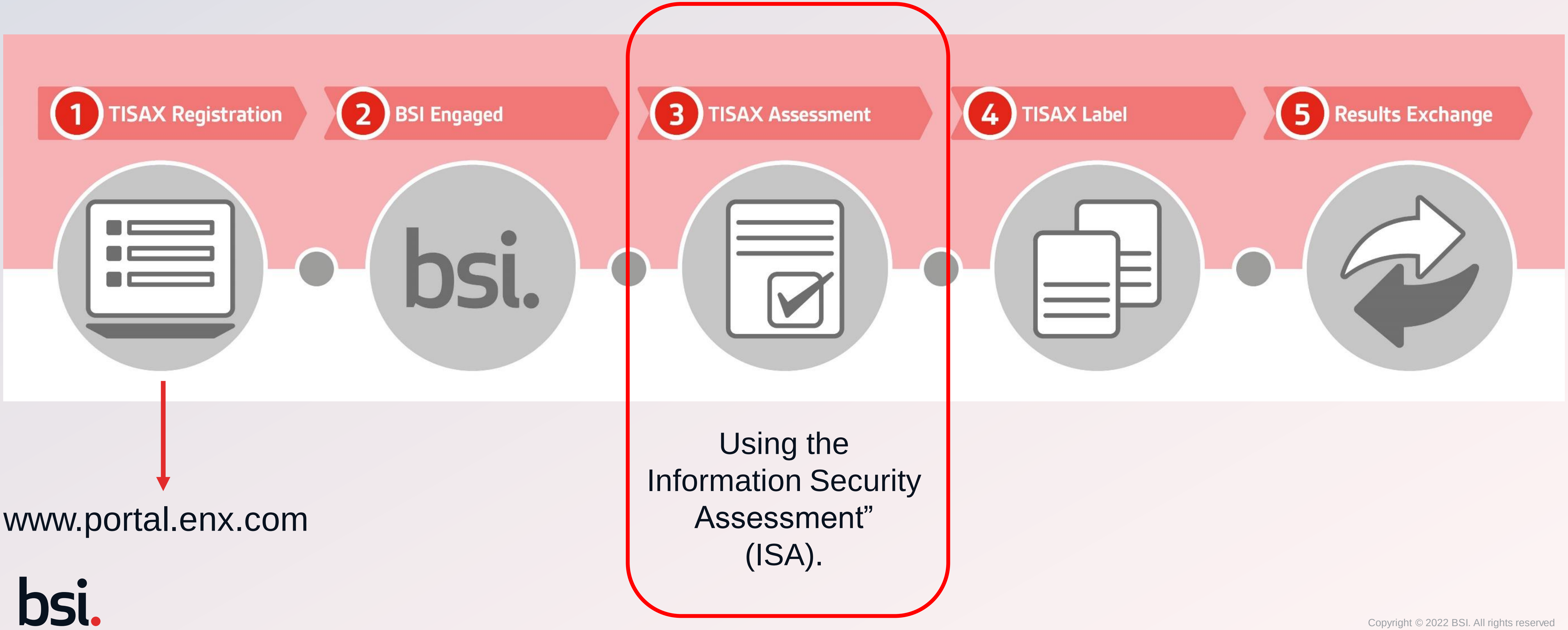
- The audit provider does all the checks as for an assessment in assessment Level 2. However, all checks will be more comprehensive, and they will thoroughly verify your self-assessment result in an in-depth on-site inspection and face-to-face interviews

# 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<br>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<br>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 |

bsi.

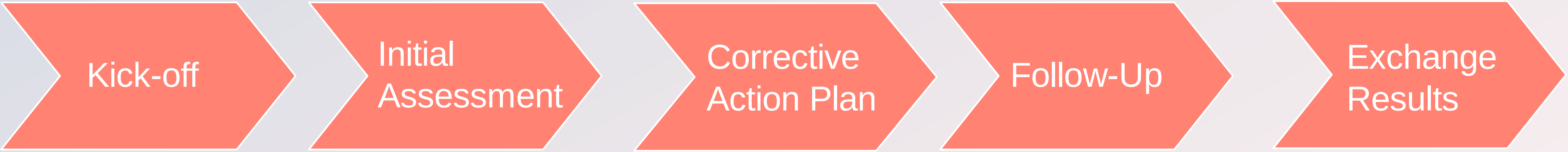
# The TISAX process – how to obtain the label



www.portal.enx.com

Using the Information Security Assessment” (ISA).

# The assessment process



## Kick-off

- Official start of the TISAX Assessment
- Communicating the whole procedure and provisions needed
- Coordinating assessment dates
- First announcement from BSI to ENX

## Initial Assessment

- Remote (AL2) or onsite (AL3) assesment
- Documentation review
- Interviews
- Closing meeting with information about the results: Clarification of potential findings and next steps

## Corrective Action Plan

- Auditee establishes and submits a Corrective Action Plan (CAP) including measurements to BSI
- BSI assesses CAP on Follow-Up, completes TISAX report

## Follow-Up

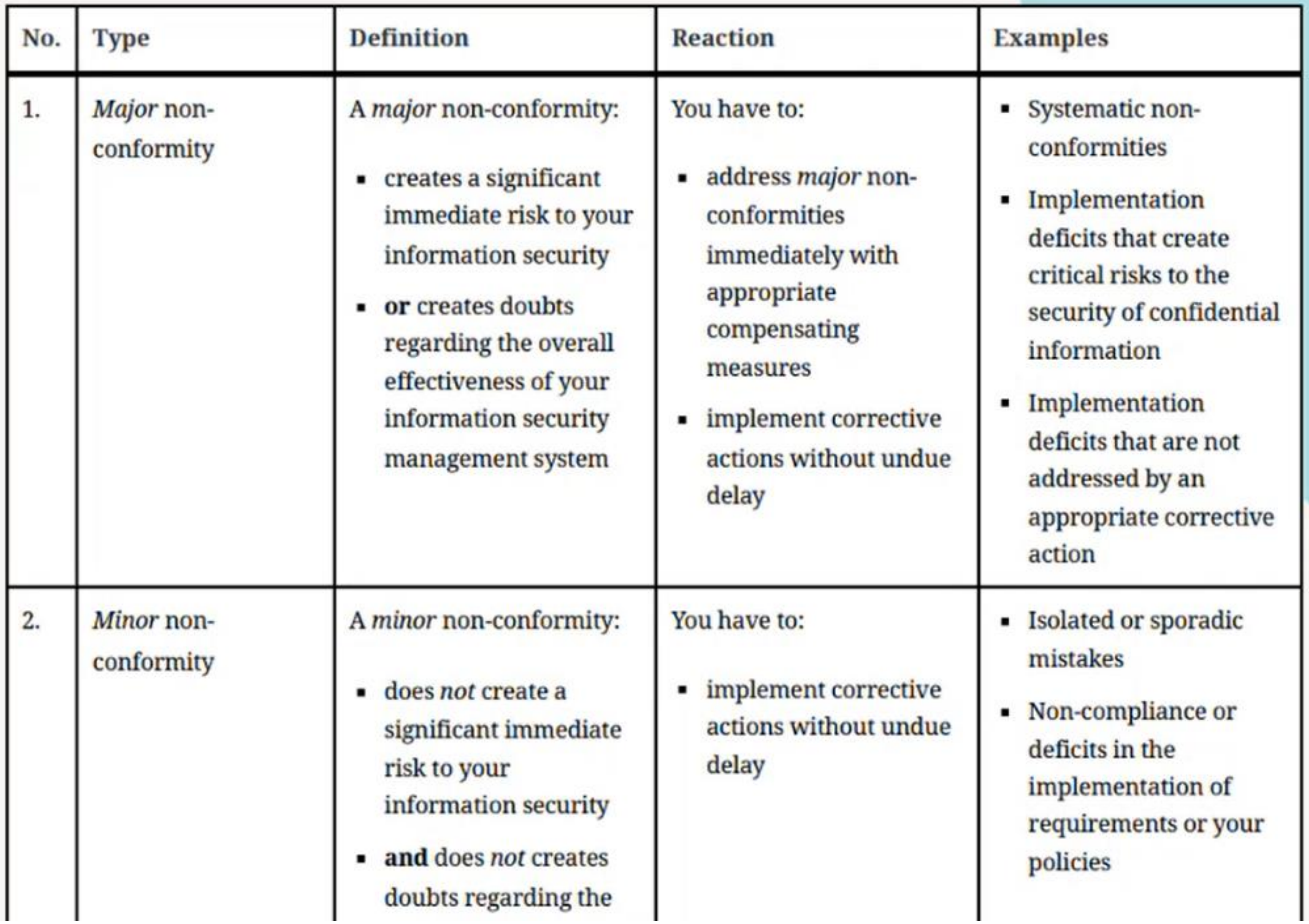
- Follow-Up is necessary to assess CAP activities
- If no findings remain, TISAX report and labels will be updated
- Otherwise CAP has to be updated
- Follow-Up assessments can be a physical or online meeting

## Exchange Results

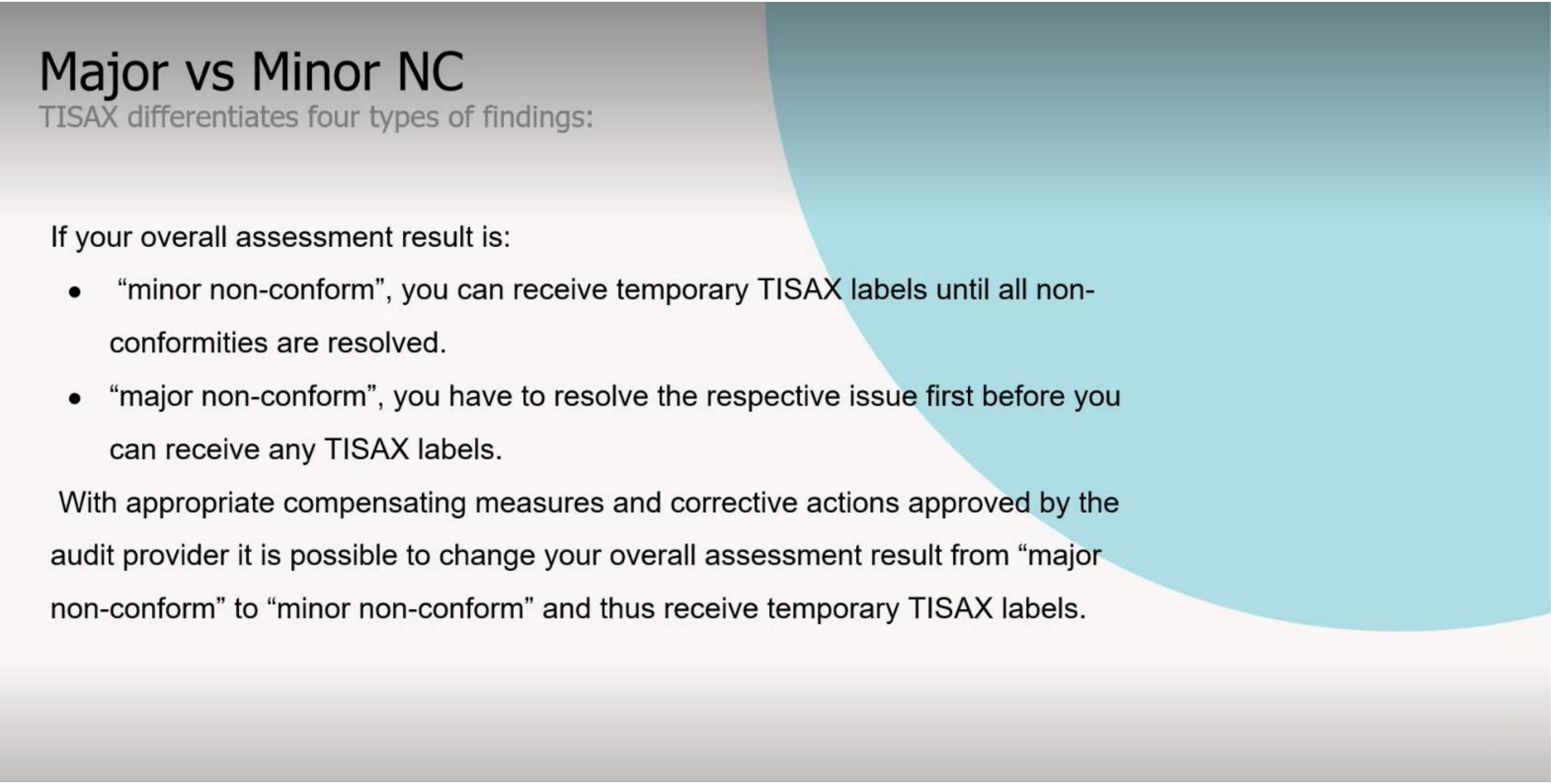
- BSI uploads first parts of TISAX report on TISAX platform
- Auditee decides who to share results to
- ENX provides TISAX labels for assessment objectives reached

# About conformity

TISAX differentiates four types of findings:



| No. | Type | Definition | Reaction | Examples |
|---|---|---|---|---|
| 1. | *Major* non-conformity | A *major* non-conformity:<br>- creates a significant immediate risk to your information security<br>- **or** creates doubts regarding the overall effectiveness of your information security management system | You have to:<br>- address *major* non-conformities immediately with appropriate compensating measures<br>- implement corrective actions without undue delay | - Systematic non-conformities<br>- Implementation deficits that create critical risks to the security of confidential information<br>- Implementation deficits that are not addressed by an appropriate corrective action |
| 2. | *Minor* non-conformity | A *minor* non-conformity:<br>- does *not* create a significant immediate risk to your information security<br>- **and** does *not* creates doubts regarding the | You have to:<br>- implement corrective actions without undue delay | - Isolated or sporadic mistakes<br>- Non-compliance or deficits in the implementation of requirements or your policies |



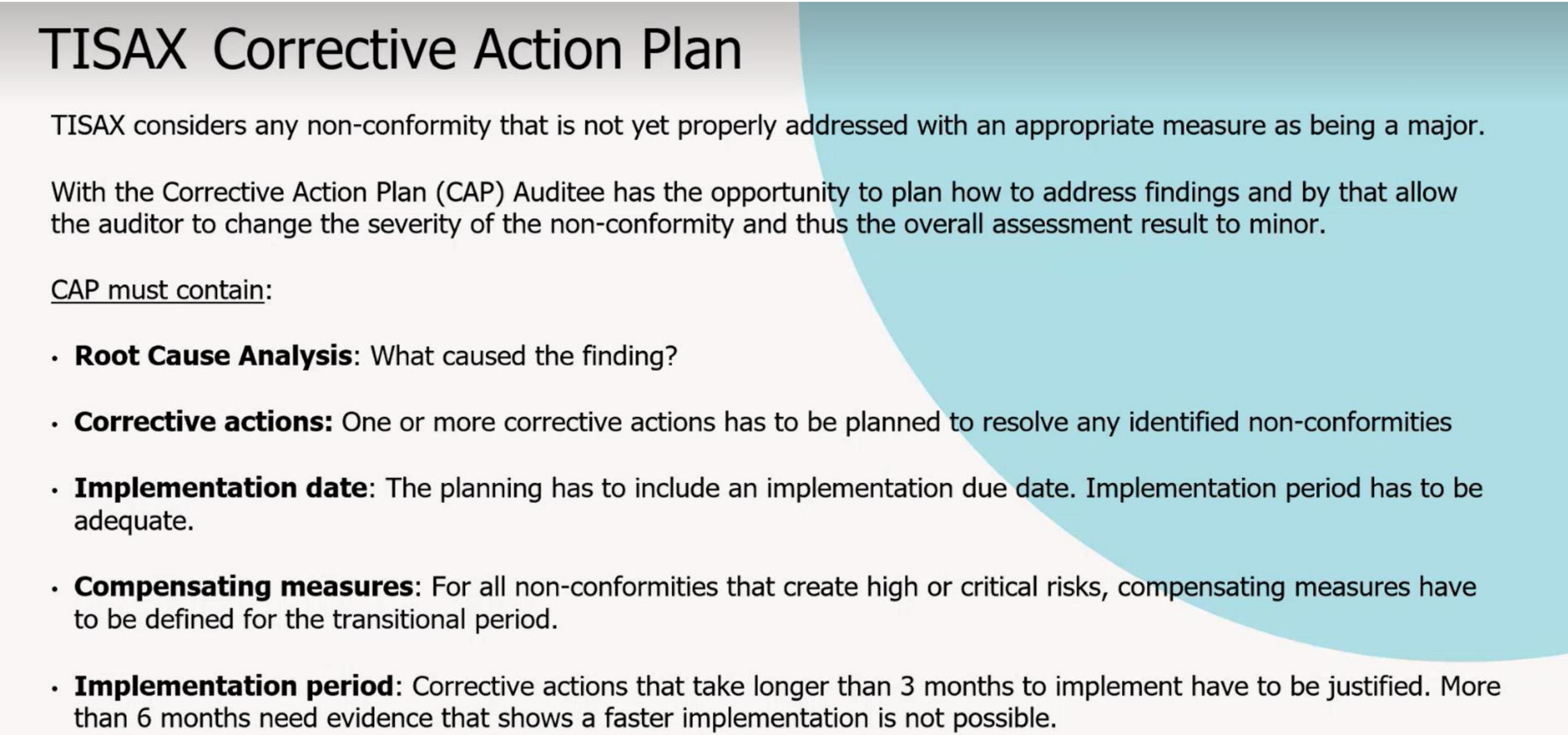
# Major vs Minor NC

TISAX differentiates four types of findings:

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.



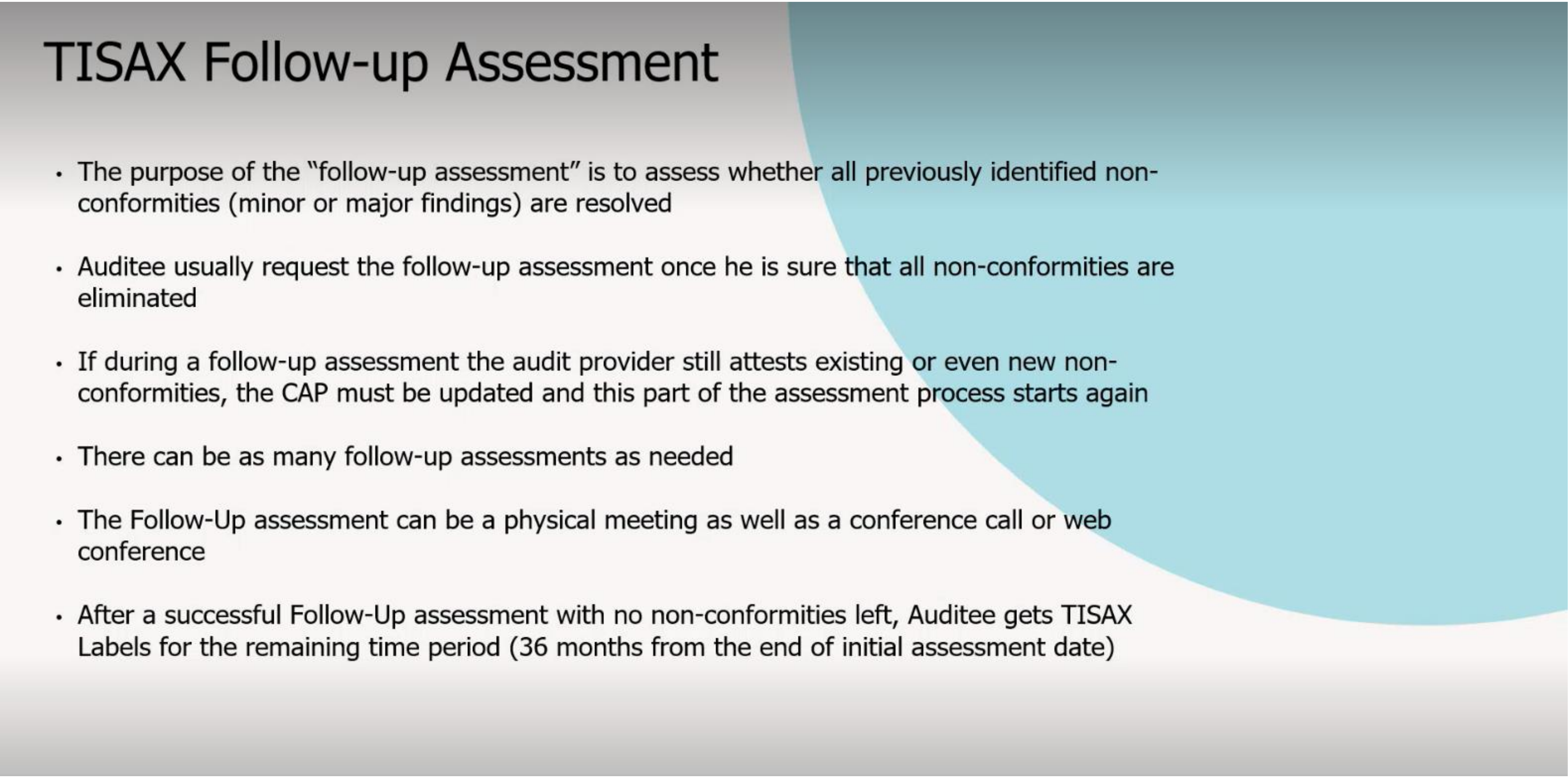
# TISAX Corrective Action Plan

TISAX considers any non-conformity that is not yet properly addressed with an appropriate measure as being a major.

With the Corrective Action Plan (CAP) Auditee has the opportunity to plan how to address findings and by that allow the auditor to change the severity of the non-conformity and thus the overall assessment result to minor.

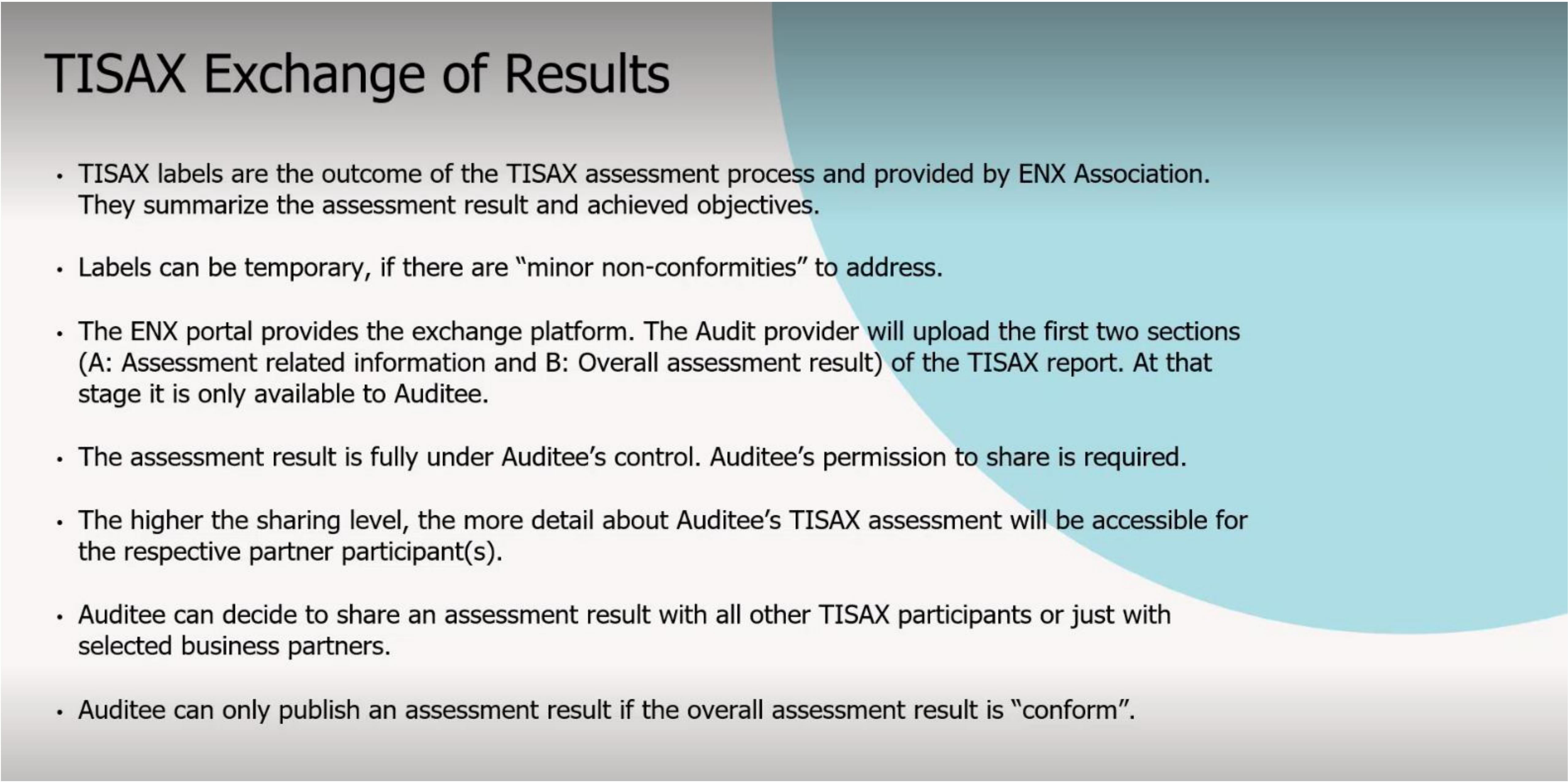
<u>CAP must contain</u>:

- **Root Cause Analysis**: What caused the finding?
- **Corrective actions:** One or more corrective actions has to be planned to resolve any identified non-conformities
- **Implementation date**: The planning has to include an implementation due date. Implementation period has to be adequate.
- **Compensating measures**: For all non-conformities that create high or critical risks, compensating measures have to be defined for the transitional period.
- **Implementation period**: Corrective actions that take longer than 3 months to implement have to be justified. More than 6 months need evidence that shows a faster implementation is not possible.



# TISAX Follow-up Assessment

- The purpose of the “follow-up assessment” is to assess whether all previously identified non-conformities (minor or major findings) are resolved
- Auditee usually request the follow-up assessment once he is sure that all non-conformities are eliminated
- If during a follow-up assessment the audit provider still attests existing or even new non-conformities, the CAP must be updated and this part of the assessment process starts again
- There can be as many follow-up assessments as needed
- The Follow-Up assessment can be a physical meeting as well as a conference call or web conference
- After a successful Follow-Up assessment with no non-conformities left, Auditee gets TISAX Labels for the remaining time period (36 months from the end of initial assessment date)



# TISAX Exchange of Results

- TISAX labels are the outcome of the TISAX assessment process and provided by ENX Association. They summarize the assessment result and achieved objectives.

- Labels can be temporary, if there are “minor non-conformities” to address.

- The ENX portal provides the exchange platform. The Audit provider will upload the first two sections (A: Assessment related information and B: Overall assessment result) of the TISAX report. At that stage it is only available to Auditee.

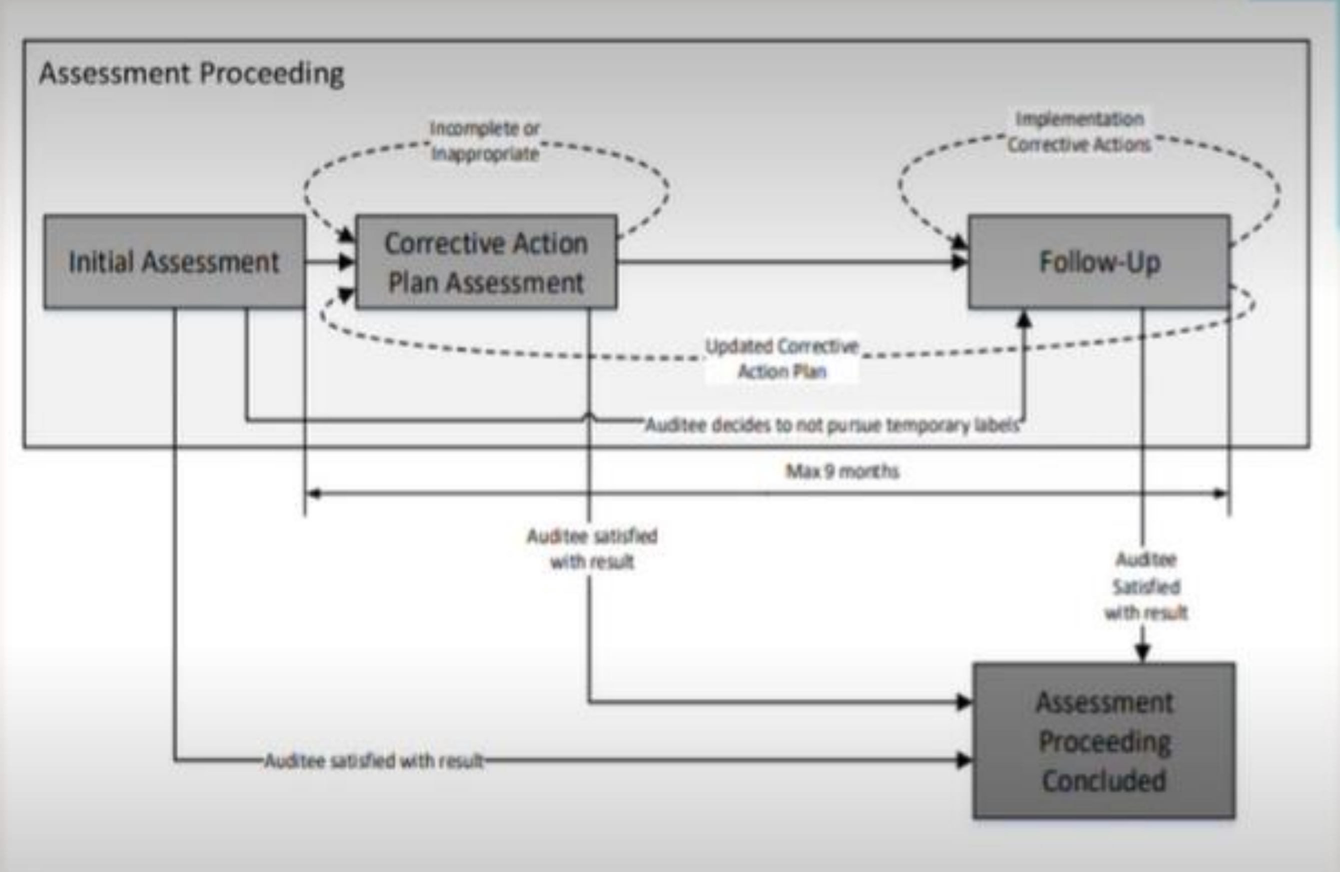
- The assessment result is fully under Auditee’s control. Auditee’s permission to share is required.

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

- Auditee can decide to share an assessment result with all other TISAX participants or just with selected business partners.

- Auditee can only publish an assessment result if the overall assessment result is “conform”.

# TISAX Assessment Proceedings

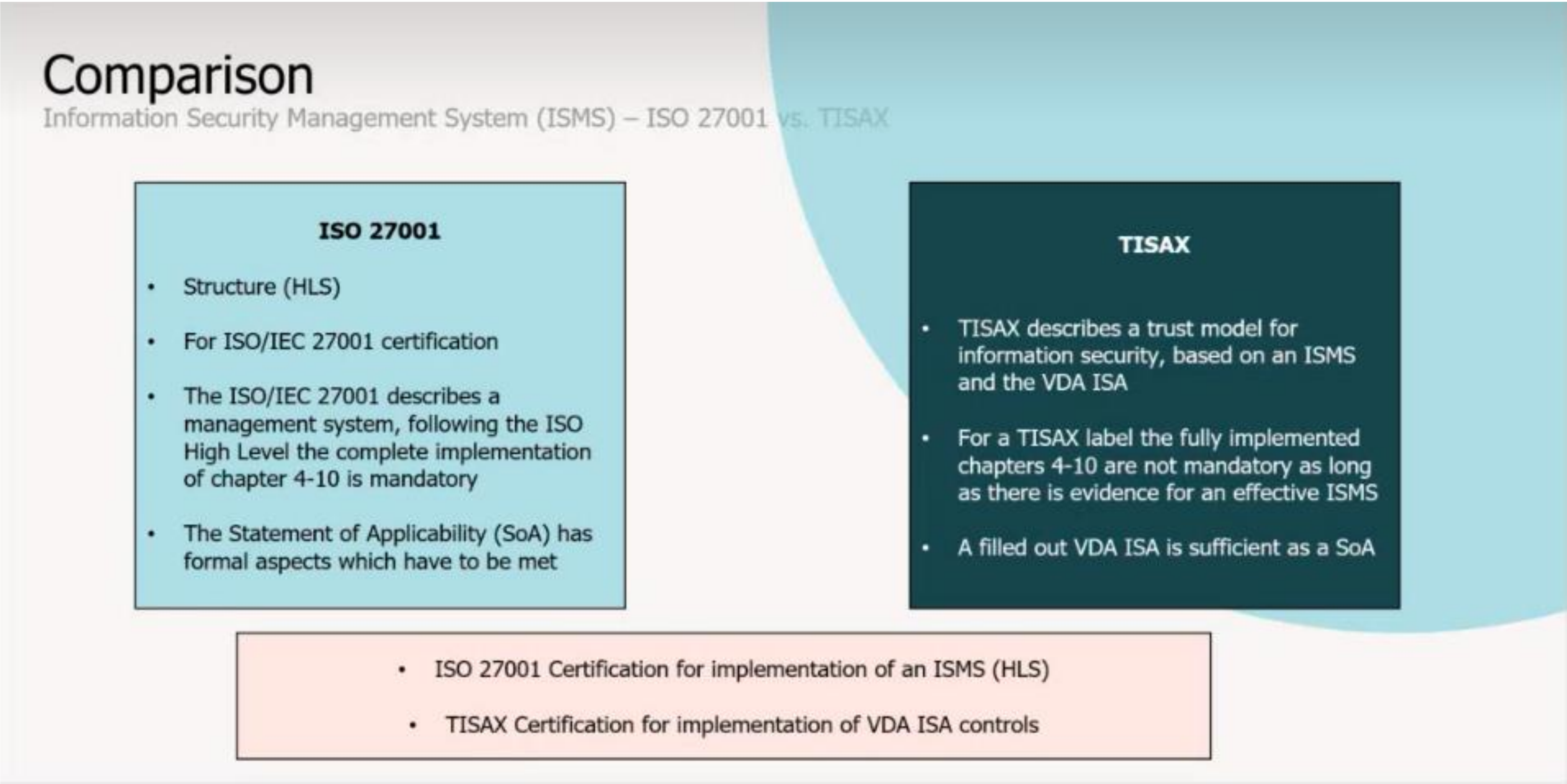


Assessment Proceeding
Incomplete or Inappropriate
Implementation Corrective Actions
Initial Assessment
Corrective Action Plan Assessment
Follow-Up
Updated Corrective Action Plan
Auditee decides to not pursue temporary labels
Max 9 months
Auditee satisfied with result
Auditee Satisfied with result
Auditee satisfied with result
Assessment Proceeding Concluded

- The Assessment starts with Initial Assessment
- If result of Initial Assessment is Conform, then TISAX label is issued and no further actions required
- If result of the Initial Assessment is Non-conform, then auditee enters Corrective Action Phase.
- The maximum time for implementing corrective actions is 9 months (starting from the initial assessment end date)
- Follow-up assessment may be required during this Phase
- Once all corrective actions are implemented and verified by the TISAX auditor, TISAX label will be issued on the ENX platform
- TISAX label is valid for 3 years and there is no surveillance audits during this period.

# Audit part

## TISAX Label program .VS. ISMS certification program



# Comparison

Information Security Management System (ISMS) – ISO 27001 vs. TISAX

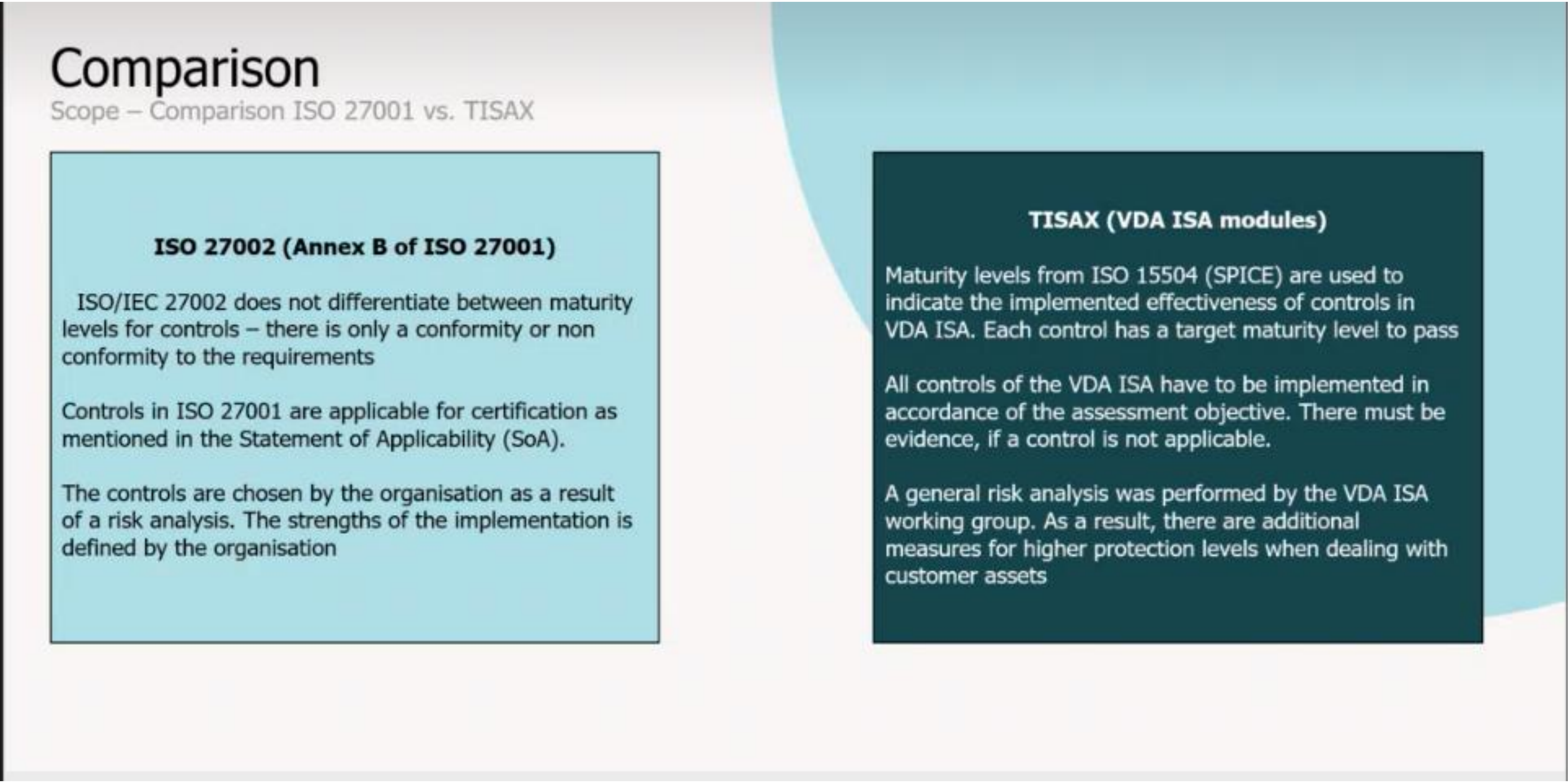
**ISO 27001**

- Structure (HLS)
- For ISO/IEC 27001 certification
- The ISO/IEC 27001 describes a management system, following the ISO High Level the complete implementation of chapter 4-10 is mandatory
- The Statement of Applicability (SoA) has formal aspects which have to be met

**TISAX**

- TISAX describes a trust model for information security, based on an ISMS and the VDA ISA
- For a TISAX label the fully implemented chapters 4-10 are not mandatory as long as there is evidence for an effective ISMS
- A filled out VDA ISA is sufficient as a SoA

- ISO 27001 Certification for implementation of an ISMS (HLS)
- TISAX Certification for implementation of VDA ISA controls



# Comparison

## Scope – Comparison ISO 27001 vs. TISAX

**ISO 27002 (Annex B of ISO 27001)**

ISO/IEC 27002 does not differentiate between maturity levels for controls – there is only a conformity or non conformity to the requirements

Controls in ISO 27001 are applicable for certification as mentioned in the Statement of Applicability (SoA).

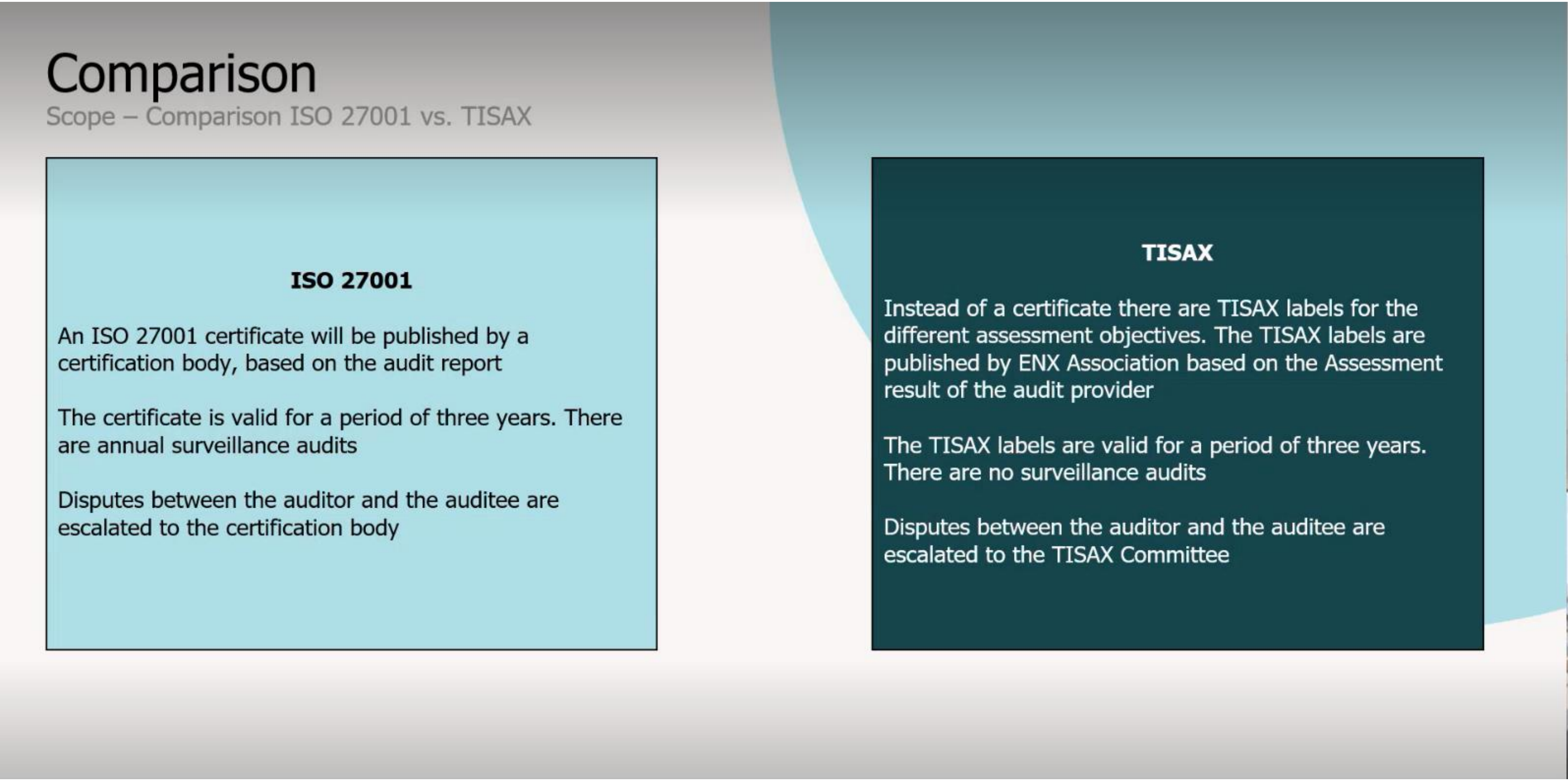
The controls are chosen by the organisation as a result of a risk analysis. The strengths of the implementation is defined by the organisation

**TISAX (VDA ISA modules)**

Maturity levels from ISO 15504 (SPICE) are used to indicate the implemented effectiveness of controls in VDA ISA. Each control has a target maturity level to pass

All controls of the VDA ISA have to be implemented in accordance of the assessment objective. There must be evidence, if a control is not applicable.

A general risk analysis was performed by the VDA ISA working group. As a result, there are additional measures for higher protection levels when dealing with customer assets



# Comparison

Scope – Comparison ISO 27001 vs. TISAX

**ISO 27001**

An ISO 27001 certificate will be published by a certification body, based on the audit report

The certificate is valid for a period of three years. There are annual surveillance audits

Disputes between the auditor and the auditee are escalated to the certification body

**TISAX**

Instead of a certificate there are TISAX labels for the different assessment objectives. The TISAX labels are published by ENX Association based on the Assessment result of the audit provider

The TISAX labels are valid for a period of three years. There are no surveillance audits

Disputes between the auditor and the auditee are escalated to the TISAX Committee

# ● 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 |
|---|---|
| IATF | ENX® |
| Quality Management System | Information Security Management System |
| IATF Certificate | TISAX Label |
| No Exchange report | Exchange report |

# Contact us

www.bsigroup.com/th-TH/

BSI Thailand

acinfotec.com

ACinfotec