CYTURUS®

Your Path to TISAX Success

Introduction

As organizations embrace digital transformation and face an increasingly complex threat landscape, ensuring robust and effective information security practices is paramount.

The TISAX (Trusted Information Security Assessment Exchange) certification has emerged as a recognized standard for evaluating and validating an organization's information security management system. However, the journey towards TISAX certification is not without its challenges.

Here we will explore the hurdles that companies encounter when seeking TISAX certification. From understanding the intricate requirements to allocating resources, conducting gap analysis, and navigating multiple standards, companies face a range of obstacles. We will delve into each of these hurdles and provide insights on how organizations can overcome them to achieve TISAX certification successfully.

By addressing these challenges head-on, companies can enhance their cybersecurity posture, gain a competitive edge, and demonstrate their commitment to protecting sensitive information.

History and Scope

TISAX (Trusted Information Security Assessment Exchange) certification was established by the German Association of the Automotive Industry (VDA) in 2017. Originally designed for the automotive industry, TISAX certification has gained recognition as a standard for assessing and validating information security management systems.

Organizations seek TISAX certification to demonstrate their commitment to information security and meet the stringent requirements set by automotive manufacturers. It helps build trust and confidence among stakeholders, ensuring the secure handling of sensitive data and protecting against cyber threats.

TISAX certification is typically required for organizations that handle sensitive information and collaborate with automotive manufacturers, suppliers, or other stakeholders in the automotive industry. This includes companies involved in areas such as manufacturing, engineering, research and development, and IT services.

The TISAX perspective is one that looks at the security of the information being processed in relation to the CIA triad: confidentiality, integrity, and availability. In addition, it takes into consideration the level of sensitivity of the information when determining what type and scope of assessment is needed. This means that the way an organization is assessed may be a little different than what we've been used to, which can cause a lot of confusion.

Preparation is Key

Before starting this journey, organizations must familiarize themselves with the TISAX framework, including the assessment criteria, control objectives, and requirements. This involves understanding the specific security controls and measures that need to be implemented.

Navigating the maze of assessment registration requirements presents an elevated learning curve. Considerations include:

1. **Understanding TISAX Scoping:**

   Most organizations will fall into the Standard Scope. This is the basis of all TISAX assessments and is what other TISAX participants will accept. Different from the way an organization scopes for ISO 270001, the scope of the TISAX assessment is predefined and can be smaller than the scope of your ISMS. But it must always be within the scope of your ISMS.

   > ***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.***[1]

[1] *Taken from Section 4.3.2.2 of the TISAX Participant Handbook*

Preparation, cont.

2. **Scoping Locations:**

   Depending on the geographic location and number of locations, an organization may choose to only include those that are required to be included in the defined scope (if the TISAX requirement came from a partner), or group locations based upon the level of assessment needed (to be grouped, all locations must have the same Assessment Objectives).

   Two additional location scoping choices are available to organizations that may decrease the monetary and time investment when certifying multiple locations: S-SGA and R-SGA. These are sample based and rotating schedule assessments. However, due care must be taken when choosing these routes as the central ISMS will be assessed in more detail and requires additional requirements are met.

3. **Assessment Levels:**

   Rather than dictate an assessment objective, a TISAX partner may require a certain "assessment level".

   a. **AL1** – Self-Assessment only: no evidence or on-site inspection will be required.

   b. **AL2** – This level will include the self-assessment, a 3rd party will conduct a "plausibility" re view of the evidence, interviews may be conducted online, and on-site inspection is only if requested.

   c. **AL3** – Required for all Prototype Facilities: includes the self-assessment, a 3rd party thorough review of all evidence, interviews conducted on-site and in-person along with an on-site inspection.

Preparation, cont.

4. **Assessment Objectives:**

   There are currently 12 objective levels. An organization may select multiple levels, but at least one objective must be chosen at registration. These levels cover different information security objectives as well as objectives for prototype facilities and those with data protection requirements (e.g., GDPR). **NOTE: ISA 6 makes minor changes to objectives effective for all new assessments after April 1, 2024.**

To better understand the registration and assessment process, download the full TISAX Participant Handbook online at: [https://www.enx.com/handbook/tisax-participant-handbook.html#ID6763.](https://www.enx.com/handbook/tisax-participant-handbook.html#ID6763)

[2] *Section 4.3.3.5 of the TISAX Participant Handbook notes:*

> *Plausibility check vs. verification*
>
> *Oversimplified, a plausibility check is checking for whether something exists and looks right. In contrast, a verification means really checking that something is what it claims to be.*

Identify your TISAX Maturity

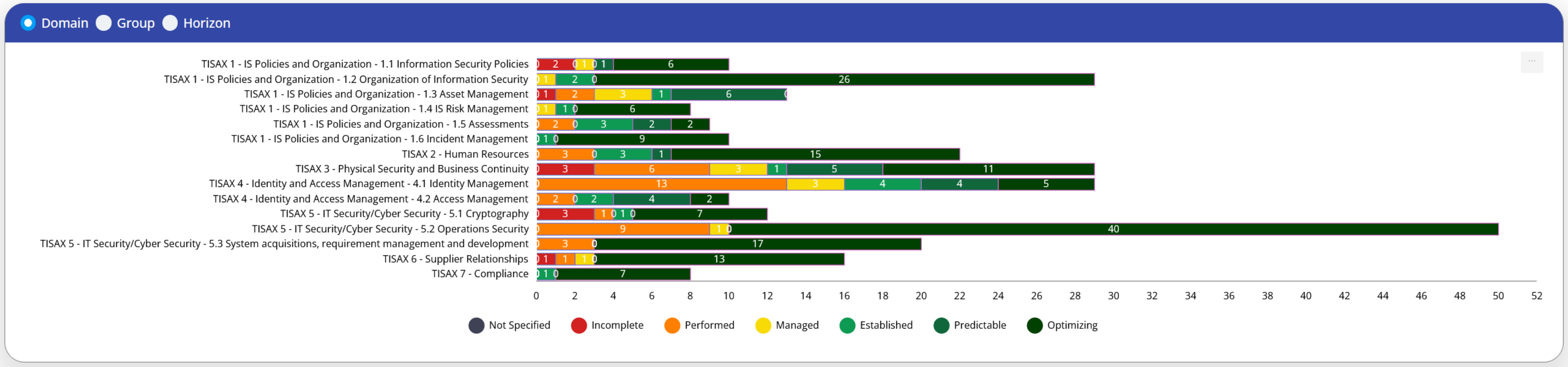
There are several phases to complete for an organization to successfully pass the assessment and receive their TISAX label:

1. **Conducting a Gap Analysis:** Organizations need to conduct a thorough assessment of their existing information security practices and compare them against the documented TISAX requirements. This helps identify gaps and deficiencies that require improvement to meet the certification standards.

2. **Implementing Information Security Measures:** To achieve TISAX certification, organizations must implement robust information security measures that align with the TISAX control objectives. This requirement includes establishing policies, procedures, and technical controls to protect sensitive information and mitigate cyber risks.

3. **Documentation and Evidence Gathering:** Organizations need to compile and organize attestation documentation that demonstrates their compliance with TISAX requirements. This can include policies, procedures, risk assessments, incident response plans, and evidence of the implementation of security controls.

Although an organization might have completed a similar work effort for another certification standard, the readiness assessment for TISAX certification must look at the information systems, associated policies, and attestation evidence based upon ALL the requirements listed for the requisite TISAX assessment level. These requirements are sometimes beyond the previous certification scope.


● Domain ○ Group ○ Horizon
TISAX 1 - IS Policies and Organization - 1.1 Information Security Policies
0 2 0 1 0 1 6
TISAX 1 - IS Policies and Organization - 1.2 Organization of Information Security
0 1 2 0 26
TISAX 1 - IS Policies and Organization - 1.3 Asset Management
0 1 2 3 1 6 0
TISAX 1 - IS Policies and Organization - 1.4 IS Risk Management
0 1 1 0 6
TISAX 1 - IS Policies and Organization - 1.5 Assessments
0 2 0 3 2 2
TISAX 1 - IS Policies and Organization - 1.6 Incident Management
0 1 0 9
TISAX 2 - Human Resources
0 3 0 3 1 15
TISAX 3 - Physical Security and Business Continuity
0 3 6 3 1 5 11
TISAX 4 - Identity and Access Management - 4.1 Identity Management
0 13 3 4 4 5
TISAX 4 - Identity and Access Management - 4.2 Access Management
0 2 0 2 4 2
TISAX 5 - IT Security/Cyber Security - 5.1 Cryptography
0 3 1 0 1 0 7
TISAX 5 - IT Security/Cyber Security - 5.2 Operations Security
0 9 1 0 40
TISAX 5 - IT Security/Cyber Security - 5.3 System acquisitions, requirement management and development
0 3 0 17
TISAX 6 - Supplier Relationships
0 1 1 1 0 13
TISAX 7 - Compliance
0 1 0 7
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52
● Not Specified ● Incomplete ● Performed ● Managed ● Established ● Predictable ● Optimizing

Almost to the Finish Line

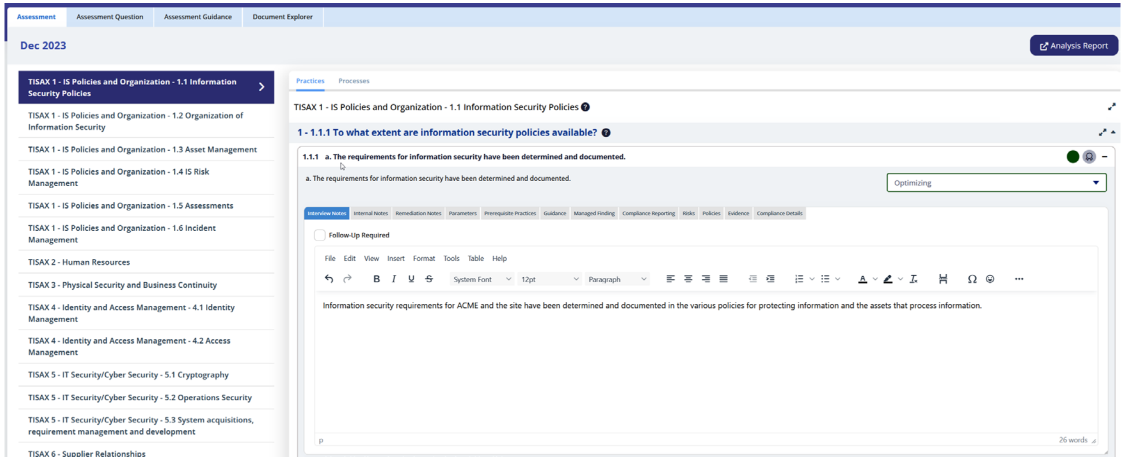
Third-Party Assessment

TISAX certification involves a third-party assessment conducted by accredited auditors. Prior to formally registering for certification, an organization should be well-prepared to engage with the auditors, provide access to in-scope systems and data for the assessment, and address any findings or recommendations.

The registration process itself can sometimes be arduous.

- Review and choose your assessment company.

  Remember that the contract and payment with the assessment company is outside the ENX portal so additional time may be needed to complete the steps before an assessment date can be scheduled.
- Choose your scope.
- Group your locations.
- Gather the site-specific details in advance and have them ready when browsing to the ENX Portal.



Dec 2023

- TISAX 1 - IS Policies and Organization - 1.1 Information Security Policies
- TISAX 1 - IS Policies and Organization - 1.2 Organization of Information Security
- TISAX 1 - IS Policies and Organization - 1.3 Asset Management
- TISAX 1 - IS Policies and Organization - 1.4 IS Risk Management
- TISAX 1 - IS Policies and Organization - 1.5 Assessments
- TISAX 1 - IS Policies and Organization - 1.6 Incident Management
- TISAX 2 - Human Resources
- TISAX 3 - Physical Security and Business Continuity
- TISAX 4 - Identity and Access Management - 4.1 Identity Management
- TISAX 4 - Identity and Access Management - 4.2 Access Management
- TISAX 5 - IT Security/Cyber Security - 5.1 Cryptography
- TISAX 5 - IT Security/Cyber Security - 5.2 Operations Security
- TISAX 5 - IT Security/Cyber Security - 5.3 System acquisitions, requirement management and development
- TISAX 6 - Supplier Relationships

TISAX 1 - IS Policies and Organization - 1.1 Information Security Policies

1 - 1.1.1 To what extent are information security policies available?

1.1.1 a. The requirements for information security have been determined and documented.

a. The requirements for information security have been determined and documented.

Optimizing

□ Follow-Up Required

Information security requirements for ACME and the site have been determined and documented in the various policies for protecting information and the assets that process information.

RECOMMENDATION: get legal and contracts and procurement involved in the registration process early. There are payments due to ENX as well as the company chosen to perform the assessment. If your company is slow to pay invoices or requires a long procurement process, this can stall your certification schedule before it starts.

Crossing the Finish Line

Ongoing Compliance and Maintenance is a Requirement

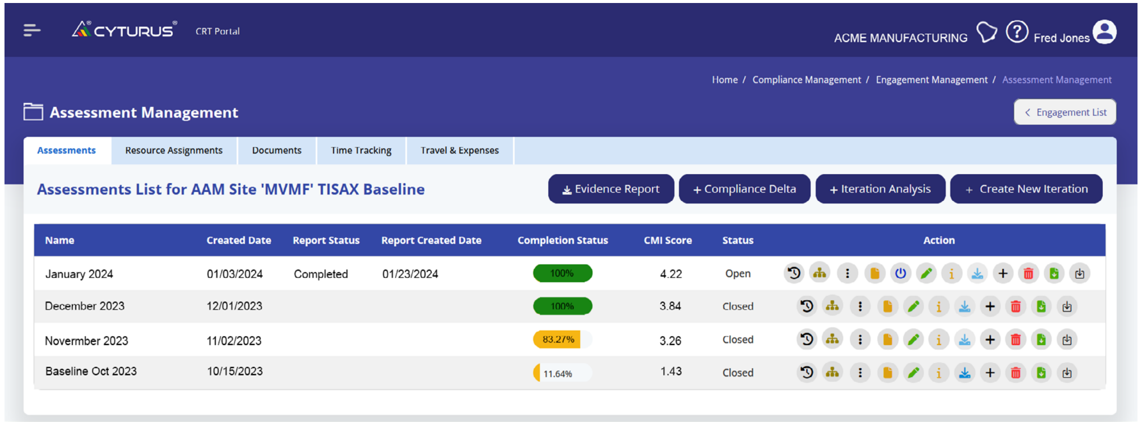
TISAX certification is not a one-time achievement. Organizations must maintain ongoing compliance with TISAX requirements, regularly review and update their information security practices, and be prepared for periodic reassessments to ensure continued TISAX certification.

The Cyturus Difference

Cyturus can assist your organization be prepared for these aspects. We streamline the path towards TISAX certification, strengthen your information security posture, and assist your organization in establishing yourself as trusted partner in the automotive industry.

Cyturus has assisted companies successfully transverse the TISAX landscape. Utilizing our Compliance and Risk Tracker (CRT) platform, Cyturus significantly reduces the amount of time to review and answer the TISAX requirements as well as having the ability to tie evidence to specific practices. For the assessor, the CRT platform reduces the time for evidence review by up to 80%.[3]

In addition, the CRT will show the organization’s maturity over time and allows for instant status reporting using iteration analysis across a length of time or by simply showing systemic deficiencies across the organization to better prioritize workloads and budgets.



Assessments List for AAM Site 'MVMF' TISAX Baseline

Name	Created Date	Report Status	Report Created Date	Completion Status	CMI Score	Status	Action
January 2024	01/03/2024	Completed	01/23/2024	100%	4.22	Open	
December 2023	12/01/2023			100%	3.84	Closed	
Novermber 2023	11/02/2023			83.27%	3.26	Closed	
Baseline Oct 2023	10/15/2023			11.64%	1.43	Closed	

[3] *Based upon the time for evidence review as noted by CMMC C3PAO RedSpin when utilizing the Cyturus CRT as opposed to the manual evidence review required in standard flat file repositories like SharePoint.*