TISAX® Assessment Report

Corrective Action Plan Assessment

U-Shin France SASU

S15XV0

AXH7MK-1

10.02.2023

Version 1.0

Initial Remarks

This Assessment Report and its underlying assessment was created by qualified experts of an TISAX audit provider. It expresses professional judgement of the effectiveness of control procedures based on the current state of implementation and in accordance to the Audit Provider Criteria and Assessment Requirements (ACAR) of the Trusted Information Security Assessment Exchange (TISAX) as defined and published by ENX Association at the time of the issuance of this report.

The Trusted Information Security Assessment Exchange (TISAX) is operated and governed by ENX Association. TISAX was created to provide commonly accepted assessments based on the ISA control catalogue conducted by trustworthy competing audit providers. Detailed information about TISAX can be found at http://www.enx.com/tisax/.

This Assessment Report is intended exclusively for use within TISAX. All distribution or exchange of TISAX Assessment Results must follow the rules for information exchange established for TISAX Participants and TISAX Audit Providers within the applicable TISAX agreements and guidelines.

No exchange of TISAX Assessment Results outside the defined TISAX information exchange proceedings or exchange with third parties outside the TISAX shall take place. Please be aware that certain rights provided by the applicable TISAX legal framework may cease when exchanging TISAX Assessment Results outside the set guidelines.

The underlying assessment engagement is not designed to detect all weaknesses in control procedures because it is not performed continuously throughout the period and the checks performed on the control procedures are on a sample basis. As such, even though checks are conducted with due diligence, misstatements due to errors or fraud may occur and go undetected.

Additionally, the assessment was based on the situation at the day of the assessment and does not account for any changes in the future. Any projections of any evaluation to future periods are subject to the risk that the report may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate.

Report Structure

This report is structured as follows:

A. Assessment Related Information
B. Summarized Results
C. Assessment Result Summary
D. Maturity Levels of VDA ISA (Result Tab)
E. Detailed Assessment Results

The structure and headlines reflect different levels of possible disclosure regarding its content towards other TISAX Participants.

Starting with general information about the assessment (A. Assessment-Related Information), it spans from a summary of results (B. Summarized Results, C. Assessment Result Summary) to the very details of the assessment (D. Maturity Levels of ISA and E. Detailed Assessment Results).

A. Assessment Related Information

A.1 Assessment Scope

TISAX® Scope-ID	S15XV0
Scope Type	☒ Standard Scope 2.0 *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.* ☐ Custom Extended Scope ☐ Full Custom Scope
Assessment Objectives	☐ Handling of Information with High Protection Level ☐ High Availability ☒ Handling of Information with Very High Protection Level ☒ Very High Availability ☒ Handling of Prototype Components and Parts ☐ Handling of Prototype Vehicles ☐ Use of Test Vehicles ☐ Events and Photo Shootings with Objects in Need of Protection ☐ Handling of Personal Data according to article 28 GDPR (“processor”) ☐ Handling with Special Categories of Personal Data (article 9 GDPR) according to article 28 GDPR (“processor”)
Assessment Requirements	ACAR – TISAX Specification of Assessment Version 2.1: Family-ID: ISA, Version 5.1

A.2 Assessed Locations

Company Name	Address	Location-ID	Contact Person
U-Shin France SASU	4 Quai de la Jonction 58000 Nevers Cedex Frankreich	LVM8ZH	Vallet, David david.vallet@g-ushin.com

The auditor confirms that all information above is verified to be accurate.

A.2.1 Initial Assessment

TISAX® Assessment-ID	AXH7MK-1
Assessment Level	AL3
Assessment Method	☐ Plausibility check of self-assessment using evidence and documentation ☐ Detailed evaluation of evidence ☒ Interviews with persons involved in the processes of the auditee ☒ On-site Inspection ☐ Video based remote site inspection
Date of Kick-Off Meeting	13.12.2022
Date of Opening Meeting	31.01.2023
Date of Closing Meeting (Effective Date)	06.02.2023
Consent of Auditee	The auditee ☒ unqualifiedly agrees on the documented conclusions. ☐ qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

A.2.2 Corrective Action Plan Assessment

TISAX® Assessment-ID	AXH7MK-2
Corrective Action Plan Date	06.02.2023
Consent of Auditee	The auditee ☒ unqualifiedly agrees on the documented conclusions. ☐ qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

Authors

Auditor
Helbig, Christopher
Quality Assurance
Trommer, Tanja

B. Summarized Results

B.1 Initial Assessment

After the initial assessment an average maturity level of 2,64 was calculated.

B.2 Corrective Action Plan Assessment

Based on the observations during the corrective action plan assessment the overall assessment of the scope is:

☐ Conform

☒ Minor non-conform (only minor non-conformities exist)

- ☒ All minor non-conformities have defined corrective actions. Latest corrective action is due on 06.07.2023 (temporary labels may be issued until this date).

☐ Major Non-conform

In total, 0 major and 13 minor non-conformities to the assessed catalogue were identified.

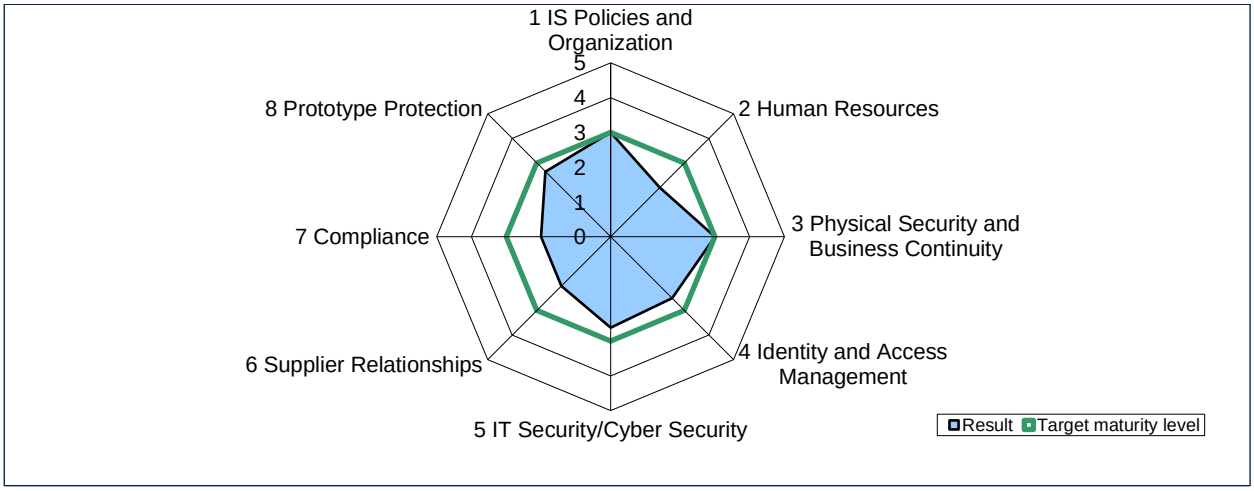
A corrective action plan was presented by the auditee to the auditor during the initial assessment.

The corrective actions planned by the auditee, the time planning and implemented compensating measures within the schedule were found to be appropriate.

C. Assessment Result Summary

C.1 Initial Assessment

The individual areas of the initial maturity levels can be found in the spider web diagram below.



C.2 Corrective Action Plan Assessment

The major and/or minor non-conformities, as applicable, were identified in the following Areas:

No.	Area	Number of major non-conformities	Number of minor non-conformities
1	IS Policies and Organization	0	0
2	Human Ressources	0	1
3	Physical Security and Business Continuity	0	0
4	Identity and Access Management	0	2
5	IT Security / Cyber Security	0	2
6	Supplier Relationships	0	2
7	Compliance	0	1
8	Prototype Protection	0	5
9	Data Protection	N/A	N/A

D. Maturity Levels of ISA (Result Tab)

D.1 ISMS

Based on the current status of implementation, the following maturity levels result for the controls listed in the ISMS Area:

No.	Control Question	Target maturity level	Result
1	***IS Policies and Organization***		
1.1	***Information Security Policies***		
1.1.1	To what extent are information security policies available?	3	**3**
1.2	***Organization of Information Security***		
1.2.1	To what extent is information security managed within the organization?	3	**3**
1.2.2	To what extent are information security responsibilities organized?	3	**3**
1.2.3	To what extent are information security requirements taken into account in projects?	3	**3**
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	**3**
1.3	***Asset Management***		
1.3.1	To what extent are information assets identified and recorded?	3	**3**
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	**3**
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	**3**
1.4	***IS Risk Management***		
1.4.1	To what extent are information security risks managed?	3	**3**
1.5	***Assessments***		
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	**3**
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	**3**
1.6	***Incident Management***		
1.6.1	To what extent are information security events processed?	3	**3**

2	***Human Resources***		
2.1.1	To what extent is the suitability of employees for sensitive work fields ensured?	3	**2**
2.1.2	To what extent is all staff contractually bound to comply with information security policies?	3	**2**
2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?	3	**2**
2.1.4	To what extent is teleworking regulated?	3	**2**
3	***Physical Security and Business Continuity***		
3.1.1	To what extent are security zones managed to protect information assets?	3	**3**
3.1.2	To what extent is information security ensured in exceptional situations?	3	**3**
3.1.3	To what extent is the handling of supporting assets managed?	3	**3**
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	3	**3**
4	***Identity and Access Management***		
4.1	***Identity Management***		
4.1.1	To what extent is the use of identification means managed?	3	**2**
4.1.2	To what extent is the user access to network services, IT systems and IT applications secured?	3	**2**
4.1.3	To what extent are user accounts and login information securely managed and applied?	3	**3**
4.2	***Access Management***		
4.2.1	To what extent are access rights assigned and managed?	3	**3**
5	***IT Security/Cyber Security***		
5.1	***Cryptography***		
5.1.1	To what extent is the use of cryptographic procedures managed?	3	**3**
5.1.2	To what extent is information protected during transport?	3	**2**
5.2	***Operations Security***		
5.2.1	To what extent are changes managed?	3	**2**

5.2.2	To what extent are development and testing environments separated from operational environments?	3	**3**
5.2.3	To what extent are IT systems protected against malware?	3	**3**
5.2.4	To what extent are event logs recorded and analyzed?	3	**2**
5.2.5	To what extent are vulnerabilities identified and addressed?	3	**2**
5.2.6	To what extent are IT systems technically checked (system audit)?	3	**3**
5.2.7	To what extent is the network of the organization managed?	3	**2**
5.3	***System acquisitions, requirement management and development***		
5.3.1	To what extent is information security considered in new or further development of IT systems?	3	**3**
5.3.2	To what extent are requirements for network services defined?	3	**3**
5.3.3	To what extent is the return and secure removal of information assets from external IT services regulated?	3	**3**
5.3.4	To what extent is information protected in shared external IT services?	3	**3**
6	***Supplier Relationships***		
6.1.1	To what extent is information security ensured among suppliers and cooperation partners?	3	**2**
6.1.2	To what extent is non-disclosure regarding the exchange of information contractually agreed?	3	**2**
7	***Compliance***		
7.1.1	To what extent is compliance with regulatory and contractual provisions ensured?	3	**3**
7.1.2	To what extent is the protection of personal data taken into account when implementing information security?	3	**1**

D.2 Handling of Prototypes

Based on the current status of implementation, the following maturity levels result for the controls listed in the Prototype Protection area:

No.	**Control Question**	**Target maturity level**	**Result**
8.1	***Physical and Environmental Security***		
8.1.1	Security concept	3	**3**

8.1.2	Perimeter security	3	**2**
8.1.3	Stability of outer skin	3	**3**
8.1.4	View and sight protection	3	**3**
8.1.5	Protection against unauthorized entry and access control	3	**2**
8.1.6	Intrusion monitoring	3	**3**
8.1.7	Visitor management	3	**3**
8.1.8	Client segregation	3	**3**
8.2	***Organizational Requirements***		
8.2.1	Non-disclosure obligations	3	**3**
8.2.2	Subcontractors	3	**2**
8.2.3	Awareness	3	**3**
8.2.4	Security classification	3	**3**
8.2.5	Access control	3	**2**
8.2.6	Film and photo regulations	3	**2**
8.2.7	Mobile video and photography devices	3	**3**
8.3	***Handling of vehicles, components and parts***		
8.3.1	Transport	3	**3**
8.3.2	Parking and storage	3	**3**
8.4	***Requirements for trial vehicles***		
8.4.1	Camouflage	3	**N/A**
8.4.2	Test and trial ground	3	**N/A**
8.4.3	Test and trial drives on public roads	3	**N/A**
8.5	***Requirements for events and shootings***		
8.5.1	Presentations and events	3	**N/A**
8.5.2	Film and photo shootings	3	**N/A**