Erstelldatum	13.01.2023
Update	16.02.2025

Herausgeber	Teilnehmer der Bewertung zur Selbsteinschätzung	
	Name	Position
SMCT MANAGEMENT concept Stefan Strößenreuther Reuthweg 11 95100 Selb		

Inhaltsverzeichnis

1. Projektvorbereitung und Scope		
1.1 TISAX Projektteam	Umgesetzt	Zufrieden
Verantwortliche(n) **benennen** (z. B. ISB-Beauftragter)	☐	☐
Kernteam definieren (IT, Recht, Management, Produktion), ggf. Prototypenschutz-Verantwortliche.	☐	☐
1.2 Umfang (Scope)	Umgesetzt	Zufrieden
Festlegen, welche **Standorte**, **Abteilungen**, **Prozesse** und **IT-Systeme** vom TISAX-Assessment betroffen sind.	☐	☐
Ermittlung der **TISAX-Labels** (z. B. Informationssicherheit, Prototypenschutz, Datenschutz), die für den Kunden relevant sind.	☐	☐
1.3 Zeitrahmen und Ressourcen	**Umgesetzt**	**Zufrieden**
Projektplan mit **Meilensteinen** (Gap-Analyse, interne Audits, Reifegrad, TISAX-Audit).	☐	☐
Budget und personelle **Kapazitäten** (Schulungen, Dokumentation, Verbesserungsmaßnahmen).	☐	☐

2. VDA ISA Anforderungskatalog		
2.1 Anforderungsniveau	Umgesetzt	Zufrieden
Prüfen, welches **Assessment Level** (z. B. AL 2, AL 3) gefordert wird.	☐	☐
Zwischenstufen definieren: Teilanforderungen (z. B. Informationssicherheit und Prototypenschutz) oder kompletter Katalog	☐	☐
2.2 Selbstbewertung (Self-Assessment)	**Umgesetzt**	**Zufrieden**
VDA ISA-Bestandteile durchgehen: **Informationssicherheit**, **Datenschutz** und ggf. **Prototypenschutz.**	☐	☐
Pro Anforderung beurteilen: Ist-Stand, Lücken (Gap), geplanter Zielzustand.	☐	☐
2.3 Dokumentation	**Umgesetzt**	**Zufrieden**
Alle Anforderungen mit **Status** (erfüllt / teilweise erfüllt / nicht erfüllt) versehen.	☐	☐
Link zur **Evidenz** (z. B. Richtlinie, Prozessbeschreibung, technische Maßnahme).	☐	☐

3. Informationssicherheit		
3.1 ISMS Struktur	Umgesetzt	Zufrieden
Dokumentierte **Informationssicherheitspolitik**, Verantwortlichkeiten (Management, ISB-Beauftragter).	☐	☐
Geltungsbereich (Scope) definiert, Verknüpfung zu anderen Systemen (ISO 27001, interne Vorgaben).	☐	☐

3.2 Risikomanagement	Umgesetzt	Zufrieden
Risikoanalyse (Assets, Bedrohungen, Schwachstellen), Priorisierung der Risiken.	☐	☐
Risikobehandlungsplan, Statement of Applicability (SoA) mit Controls aus VDA ISA.	☐	☐
3.3 Technische und organisatorische Kontrollen	**Umgesetzt**	**Zufrieden**
Firewalling, Anti-Malware, Patch-Management, Zugriffskontrolle, Datensicherungen.	☐	☐
Security-**Awareness**-Schulungen, physische Sicherheitsmaßnahmen (Zutrittskontrolle), Clean-Desk-Policy	☐	☐
3.4 Incident Management	**Umgesetzt**	**Zufrieden**
Definition von Meldestrukturen, Rollen und Eskalationswegen bei sicherheitsrelevanten Vorfällen.	☐	☐
Dokumentierte Verfahren z.B. Backup, Netzwerksicherheit, Instandhaltung IT-Geräte, Wiederanlauf, Lessons Learned usw.		

4. Prototypenschutz (Prototyp Security Requirements)		
4.1 Prozesserfassung	Umgesetzt	Zufrieden
Identifikation aller Prozesse, in denen **Prototypen** (Fahrzeugteile, Designstudien, Softwareteile) entwickelt, gelagert, transportiert oder getestet werden.	☐	☐
Verantwortlichkeiten klären: Wer hat Zugriff, wer darf Prototypen extern weitergeben?	☐	☐
4.2 Physische Sicherheit und Logistik	**Umgesetzt**	**Zufrieden**
Zugangsbeschränkungen zu Prototypenlager oder Testbereichen (Zutrittsausweise, Kameras, Sperrzonen).	☐	☐
Transportwege (z. B. Lieferanten, Kurier) mit besonderen Sicherheitsvorkehrungen (Versiegelung, GPS-Tracking)	☐	☐
4.3 Informationssicherheit	**Umgesetzt**	**Zufrieden**
Verschlüsselte Datenübertragung und Speicherung von Prototypendaten (z. B. CAD-Dateien).	☐	☐
NDAs (Non-Disclosure Agreements) für Mitarbeitende, Lieferanten und Besucher.	☐	☐
4.4 Notfall- und Abweichungsfälle	**Umgesetzt**	**Zufrieden**
Vorgehensweisen bei Verlust oder Diebstahl eines Prototypen (z. B. sofortige Meldung, Schadensbegrenzung).		
Dokumentation, Berichtspflichten gegenüber Kunden **(Automobilhersteller).**		

5. Datenschutz		
5.1 DSGVO Compliance	Umgesetzt	Zufrieden

Verzeichnis von **Verarbeitungstätigkeiten**, Rechtsgrundlagen, Löschfristen.	☐	☐
Richtlinien (z. B. Zugriffskonzept, Einwilligungsprozesse, Rechte der Betroffenen.	☐	☐
5.2 Organisatorische Maßnahmen	Umgesetzt	Zufrieden
Bestellung eines **Datenschutzbeauftragten** (wo erforderlich).	☐	☐
Awareness-Schulungen für Mitarbeitende zum Umgang mit personenbezogenen Daten.	☐	☐
5.3 Technische Maßnahmen	Umgesetzt	Zufrieden
Pseudonymisierung/Verschlüsselung, Protokollierung von Zugriffen, Datenschutz by Design/Default.		
Verfahren zur Meldung von Datenschutzverletzungen (Meldefristen, Verantwortlichkeiten.		

6. Lieferkettensicherheit		
6.1 Auswahl- und Bewertungsverfahren	Umgesetzt	Zufrieden
Checkliste oder Audit-Verfahren, um Zulieferer und Dienstleister auf TISAX-relevante Sicherheitsanforderungen zu prüfen.	☐	☐
Verträge (z. B. **SLA**, Geheimhaltungsvereinbarung) mit Sicherheitsklauseln.	☐	☐
6.2 Kontinuierliches Monitoring	Umgesetzt	Zufrieden
Lieferantenranking (Erfüllungsgrad TISAX, Auditberichte, ggf. Zertifikate)	☐	☐
Dokumentierte Eskalationswege bei **Verstößen** oder **Sicherheitsvorfällen** in der Lieferkette.	☐	☐

7. Abschluss und RE-Evaluierung		
7.1 Aktualisierung der Risikoanalyse	Umgesetzt	Zufrieden
Nach **wesentlichen Änderungen** (z. B. neue IT-Systeme, Standortverlagerungen, Personalwechsel) die Risikoanalyse anpassen.	☐	☐
Periodische **Neubewertung** (z. B. jährlich oder halbjährlich) durchführen, um neue Bedrohungen oder Schwachstellen zu berücksichtigen.	☐	☐
7.2 Beispiel Daten und Prototypen extern	Umgesetzt	Zufrieden
Klären, wie Daten (z. B. **Konstruktionspläne**) weitergegeben werden dürfen (Verschlüsselung, Minimalprinzip).	☐	☐
Bei Kooperationspartnern / Lieferanten: Physischer oder virtueller Schutz von Prototypen (z. B. besondere Lagerräume)	☐	☐

8. Implementierung und Dokumentation		
8.1 Policy- und Prozessdokumentation	Umgesetzt	Zufrieden

Informationssicherheitspolitik (inkl. Prototypenschutz), Richtlinien, Verfahrensanweisungen (z. B. Passwortvorgaben, Prototypfreigabeprozesse).	☐	☐
Klare **Versionslenkung**, Freigabeprozesse und Verantwortlichkeiten.	☐	☐
8.2 Risikomanagement	Umgesetzt	Zufrieden
Bewertung sämtlicher relevanter **Assets** inkl. Prototypen, personenbezogene Daten (falls zutreffend).	☐	☐
Risikobehandlungsplan: Maßnahmen, Verantwortliche, Termine	☐	☐
8.3 Schulung und Awareness	Umgesetzt	Zufrieden
Mitarbeitende in **sicherheitskritischen** Bereichen (z. B. Werkstatt, IT, Logistik) regelmäßig schulen und Tests durchführen.	☐	☐
Ggf. E-Learning-Plattform, interne Workshops	☐	☐

9. Interne Audits und Selbsteinschätzung		
9.1 Self-Assessment nach VDA ISA (aktuell 6)	Umgesetzt	Zufrieden
Alle Anforderungen (z. B. InfoSec, Prototypenschutz, Datenschutz) abprüfen und dokumentieren (Status: erfüllt, teilweise, nicht erfüllt).	☐	☐
Gap-Analyse: Maßnahmen zur Schließung von Lücken.	☐	☐
9.2 Interne Audits	Umgesetzt	Zufrieden
Auditprogramm erstellen (Wann? Welche Standorte? Welcher Fokus?).	☐	☐
Auditfeststellungen priorisieren und im Maßnahmenplan nachverfolgen.	☐	☐
9.3 Managementbewertung	Umgesetzt	Zufrieden
Ergebnisse der Self-Assessment und Audits an die Leitung berichten.	☐	☐
Beschlüsse (z. B. zusätzliche Ressourcen, Prozessoptimierungen) dokumentieren	☐	☐

10. Vorbereitung TISAX Assessment		
10.1 Assessment Level (AL) klären	Umgesetzt	Zufrieden
Mit Kunden oder OEM abstimmen, ob AL 2 (z. B. Hochvertrauliche Daten) oder AL 3 (erhöhte Anforderungen) gefordert wird	☐	☐
Bei Prototypenschutz: Prüfen, ob High Level Security verlangt wird	☐	☐
10.2 Externe Prüfstelle wählen	Umgesetzt	Zufrieden

Akkreditiertes Prüfinstitut (TISAX-Prüfstelle) recherchieren, Angebote einholen.	☐	☐
Terminierung für das TISAX-Audit (Stage 1: Dokumentenprüfung, Stage 2: Vor-Ort-Prüfung).	☐	☐
10.3 Finaler Check	Umgesetzt	Zufrieden
Sicherstellen, dass alle Dokumente (Richtlinien, Berichte, Nachweise) **audit-ready** sind.	☐	☐
Schlüsselpersonen (z. B. IT-Leiter, Prototypenverantwortliche) briefen, mögliche Auditfragen durchgehen.	☐	☐

11. Kontinuierliche Verbesserung		
11.1 Maßnahmenverfolgung	Umgesetzt	Zufrieden
Offene Abweichungen aus Self-Assessment oder externem TISAX-Audit priorisieren und bearbeiten.	☐	☐
KVP-Methoden (z. B. Lessons Learned) nutzen, um System kontinuierlich zu verbessern.	☐	☐
10.2 RE-Zertifizierung / RE-Assessment	Umgesetzt	Zufrieden
TISAX-Zertifikat hat eine bestimmte Gültigkeitsdauer (3 Jahre): rechtzeitig Rezertifizierung oder regelmäßige Wiederhol-Assessments planen	☐	☐
Neue Anforderungen (z. B. Updates des VDA ISA Katalogs) beobachten und ins System integrieren.	☐	☐

SMCT MANAGEMENT begleitet Unternehmen umfassend auf dem Weg zur erfolgreichen TISAX-Zertifizierung. Wir unterstützen bereits bei der Definition des Projektumfangs und helfen, die VDA-ISA-Anforderungen zu verstehen und in die eigene Organisation zu übertragen. Gemeinsam führen wir eine Gap-Analyse durch, erstellen einen strukturierten Maßnahmenplan und etablieren die erforderlichen Prozesse, um Informationssicherheit, Prototypenschutz, Datenschutz und Lieferkettensicherheit gemäß TISAX-Anforderungen nachzuweisen.

Dabei legen wir besonderen Wert auf eine praxisnahe Umsetzung: Unser Team bindet alle relevanten Abteilungen mit ein – von der IT über das Engineering bis hin zur Logistik. Wir beraten zu Risikomanagement, entwickeln Sicherheitsrichtlinien und begleiten Awareness-Schulungen, damit jedes Teammitglied seine Rolle im Sicherheitskonzept versteht. Durch unsere Erfahrung im Automobilsektor kennen wir die branchenspezifischen Erwartungen und auditieren auf Wunsch interne Prozesse, um bereits vor dem offiziellen TISAX-Audit Optimierungspotenziale aufzudecken.

Am Ende steht nicht nur ein formal erreichter Standard, sondern ein tatsächlich gelebtes Informationssicherheits- und Prototypenschutzniveau, das Vertrauen bei OEMs und Zulieferern schafft und die Wettbewerbsfähigkeit langfristig stärkt.