

Inhalt

Vorwort	XIII
Hinweis	XV
Einführung	XVII
Bedeutung von TISAX® in der Automobilindustrie	XVII
Änderungen im TISAX®-Prüfverfahren.....	XVIII
Anforderungskatalog.....	XX
Der Weg zum TISAX®-Label	XXI
① Scope definieren	XXI
② Gap-Analyse	XXII
③ Registrierung	XXIV
④ Auswahl eines akkreditierten Prüfdienstleisters.....	XXV
⑤ Kick-off-Termin	XXV
⑥ Bereitstellung der Nachweise für das Assessment	XXV
⑦ Durchführung des Assessments.....	XXVII
⑧ Bewertung.....	XXVIII
⑨ Corrective Action Plan (CAP).....	XXIX
⑩ Erhalt des TISAX®-Labels	XXIX
⑪ Nach dem Assessment ist vor dem Assessment	XXX

1	Richtlinien und Organisation der Informationssicherheit. . . .	1
1.1	Richtlinien zur Informationssicherheit.	1
1.1.1	Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?	1
1.2	Organisation der Informationssicherheit.	9
1.2.1	Inwieweit wird in der Organisation Informationssicherheit gemanagt?	9
1.2.2	Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?	13
1.2.3	Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?	19
1.2.4	Inwieweit sind die Verantwortlichkeiten zwischen organisationsfremden IT-Dienstleistern und der eigenen Organisation definiert?	22
1.3	Asset-Management	26
1.3.1	Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?	26
1.3.2	Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?	30
1.3.3	Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?	36
1.3.4	Inwieweit wird sichergestellt, dass nur evaluierte und zugelassene Software zum Verarbeiten von Informationswerten der Organisation eingesetzt wird?	40
1.4	Risikomanagement für Informationssicherheit	45
1.4.1	Inwieweit werden Informationssicherheitsrisiken gemanagt?	45
1.5	Assessment	54
1.5.1	Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?	54
1.5.2	Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?	58
1.6	Vorfall- und Krisenmanagement.	59
1.6.1	Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?	59
1.6.2	Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?	64
1.6.3	In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?	74

2	Personalmanagement	87
2.1	Sicherstellung der Einhaltung der Informationssicherheit durch Mitarbeitende	88
2.1.1	Inwieweit wird die Eignung von Mitarbeitenden für sensible Tätigkeitsbereiche sichergestellt?	88
2.1.2	Inwieweit werden alle Mitarbeitenden vertraglich zur Einhaltung der Informationssicherheitsrichtlinien verpflichtet?	91
2.1.3	Inwieweit werden Mitarbeitende hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?	95
2.1.4	Inwieweit ist mobiles Arbeiten geregelt?	98
3	Management der physischen Sicherheit	105
3.1	Informationswerte, Informationsträger, mobile IT-Geräte und Datenträger	105
3.1.1	Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?	105
3.1.2	Ersetzt durch 1.6.3, 5.2.8 und 5.2.9	115
3.1.3	Inwieweit ist der Umgang mit Informationsträgern gemanagt?	116
3.1.4	Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?	119
4	Identitäts- und Zugriffsverwaltung	123
4.1	Identitätsverwaltung	123
4.1.1	Inwieweit ist der Umgang mit Identifikationsmitteln verwaltet? ...	124
4.1.2	Inwieweit wird der Zugang von Benutzern zu IT-Diensten und IT-Systemen gesichert?	127
4.1.3	Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewendet?	133
4.2	Zugriffsverwaltung	146
4.2.1	Inwieweit werden Zugriffsrechte vergeben und verwaltet?	146
5	IT-Sicherheit/Cybersicherheit	151
5.1	Kryptografie	151
5.1.1	Inwieweit wird die Nutzung kryptografischer Verfahren verwaltet?	151
5.1.2	Inwieweit werden Informationen während der Übertragung geschützt?	156

5.2	Operation Security	161
5.2.1	Inwieweit werden Änderungen verwaltet?	161
5.2.2	Inwieweit sind Entwicklungs- und Testumgebungen von Produktivumgebungen getrennt?	164
5.2.3	Inwieweit werden IT-Systeme vor Schadsoftware geschützt?	167
5.2.4	Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?	173
5.2.5	Inwieweit werden Schwachstellen erkannt und behandelt?	178
5.2.6	Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?	181
5.2.7	Inwieweit wird das Netzwerk der Organisation verwaltet?	184
5.2.8	Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?	188
5.2.9	Inwieweit wird die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt?	198
5.3	Systemanschaffung, Anforderungsmanagement und Entwicklung	203
5.3.1	Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?	203
5.3.2	Inwieweit sind Anforderungen an Netzwerkdienste definiert?	207
5.3.3	Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?	211
5.3.4	Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?	214
6	Lieferantenbeziehungen	219
6.1	Informationssicherheit und Vertragsgestaltung mit Partnern	220
6.1.1	Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?	220
6.1.2	Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?	226
7	Compliance.	231
7.1	Rechtstreue und Konformität.	231
7.1.1	Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?	231
7.1.2	Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt?	235

8	Prototypenschutz	241
8.1	Physische und umgebungsbezogene Sicherheit	242
8.1.1	Inwieweit ist ein Sicherheitskonzept vorhanden, das Mindestanforderungen zur physischen und umgebungsbezogenen Sicherheit für den Prototypenschutz beschreibt?	242
8.1.2	Inwieweit ist Perimeterschutz vorhanden, der den unberechtigten Zutritt zu geschützten Objekten der Liegenschaften verhindert?	246
8.1.3	Inwieweit ist die Außenhaut der geschützten Gebäude in einer Form ausgeführt, die das Entfernen oder Öffnen von Außenhautkomponenten mit handelsüblichen Werkzeugen verhindert?	247
8.1.4	Inwieweit wird der Sicht- und Einblickschutz in definierte Sicherheitsbereiche sichergestellt?	248
8.1.5	Inwieweit ist der Schutz vor unbefugtem Betreten in Form einer Zugangskontrolle geregelt?	250
8.1.6	Inwieweit werden die zu sichernden Räumlichkeiten auf Einbruch überwacht?	252
8.1.7	Inwieweit ist ein dokumentiertes Besuchermanagement vorhanden?	255
8.1.8	Inwieweit ist eine Mandantentrennung vor Ort gegeben?	256
8.2	Organisatorische Anforderungen	258
8.2.1	Inwieweit liegen vertragsrechtlich gültige Geheimhaltungsvereinbarungen/-verpflichtungen vor?	258
8.2.2	Inwieweit sind Vorgaben für die Beauftragung von Unterauftragnehmern bekannt und erfüllt?	259
8.2.3	Inwieweit werden Mitarbeitende und Projektbeteiligte bezüglich des Umgangs mit Prototypen nachweislich geschult und sensibilisiert?	261
8.2.4	Inwieweit sind die Sicherheitseinstufungen des Projekts und die daraus resultierenden Maßnahmen zur Absicherung bekannt?	263
8.2.5	Inwieweit ist ein Prozess zur Zutrittsvergabe in Sicherheitsbereiche definiert?	264
8.2.6	Inwieweit sind Regelungen zur Bildaufzeichnung und zum Umgang mit erstelltem Bildmaterial vorhanden?	265
8.2.7	Inwieweit ist ein Prozess für das Mitführen und die Nutzung von mobilen Video- und Fotogeräten in definierten Sicherheitsbereichen etabliert?	267

8.3	Umgang mit Fahrzeugen, Komponenten und Bauteilen	269
8.3.1	Inwieweit werden Transporte von als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen nach den Vorgaben des Auftraggebers abgewickelt?	269
8.3.2	Inwieweit ist sichergestellt, dass als schutzbedürftig klassifizierte Fahrzeuge, Komponenten und Bauteile den Vorgaben des Auftraggebers entsprechend abgestellt/gelagert werden?	271
8.4	Anforderungen für Versuchsfahrzeuge	272
8.4.1	Inwieweit werden die vorgegebenen Regelungen zur Tarnung von den Projektbeteiligten umgesetzt?	273
8.4.2	Inwieweit werden Maßnahmen für den Schutz von freigegebenem Test- und Erprobungsgelände eingehalten/umgesetzt?	274
8.4.3	Inwieweit werden die Schutzmaßnahmen für freigegebene Test- und Erprobungsfahrten in der Öffentlichkeit eingehalten/umgesetzt?	276
8.5	Anforderungen für Veranstaltungen und Shootings	277
8.5.1	Inwieweit sind die Sicherheitsvorgaben für Ausstellungen und Veranstaltungen mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt?	278
8.5.2	Inwieweit sind die Schutzmaßnahmen für Film- und Fotoshootings mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt?	280
9	Data Protection Policies and Organization	283
9.1	Data Protection Policies	284
9.1.1	Inwieweit sind Richtlinien zum Datenschutz vorhanden?	284
9.2	Organization of Data Protection	285
9.2.1	Inwieweit sind die Verantwortlichkeiten für Datenschutz organisiert?	285
9.3	Verarbeitungsverzeichnis	287
9.3.1	Inwieweit werden Verarbeitungen identifiziert und erfasst?	287
9.4	Datenschutzfolgenabschätzung	290
9.4.1	Inwieweit wird der Umgang mit risikoreichen Verarbeitungen sichergestellt (Datenschutzfolgenabschätzung)?	290
9.5	Datenübermittlungen	293
9.5.1	Inwieweit ist die Übermittlung von Daten gemanagt?	293
9.5.2	Inwieweit werden vertragliche Vereinbarungen an Auftragnehmer und Kooperationspartner weitergegeben und deren Einhaltung überprüft?	297

9.5.3	Inwieweit werden Datenübermittlungen an Drittländer gemanagt?..	299
9.6	Umgang mit Anfragen und Vorfällen.....	300
9.6.1	Inwieweit werden Betroffenenanfragen verarbeitet?.....	300
9.6.2	Inwieweit werden Datenschutzvorfälle verarbeitet?.....	303
9.7	Human Resources.....	307
9.7.1	Inwieweit werden Mitarbeitende auf Vertraulichkeit verpflichtet?.	307
9.7.2	Inwieweit werden Mitarbeitende zum Datenschutz geschult?	308
9.8	Weisungen	310
9.8.1	Inwieweit ist der Umgang mit Weisungen in Auftrags- verarbeitungsverhältnissen gemanagt?.....	310
Abkürzungsverzeichnis		313
Anhang: Vorlagen und Checklisten		317
Nachweisliste.....		317
Dokumentenhistorie		335
Verpflichtung zur Einhaltung der Richtlinien zur Informationssicherheit		336
Lieferantenmanagement		337
Die Autorin.....		339
Index		341